DON'T!

(OR
HOW TO CARE
FOR YOUR
COMPUTER)

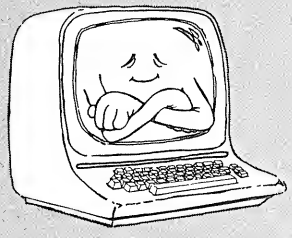
RODNAY ZAKS

SYBEX

DON'T!

Or How To Care For Your Computer

If one word does not succeed, 10,000 are of no avail.
—Chinese Proverb



DON'T!

Or How To Care For Your Computer

RODNAY ZAKS

Berkeley • Paris • Düsseldorf

CREDITS
Cover and cartoons by Daniel Le Noury
Technical illustrations by Jeanne E. Tennant
Book composition by Judy L. Wohlfrom

Library of Congress Card Number: 81-51129
ISBN 089588-065-2
First Edition 1981
Printed in the United States of America
10 9 8 7 6 5 4 3

This book
is dedicated to
the allegedly mythical trouble-free
computer

Contents

Preface

Over the past thirteen years, I have been associated with, or responsible for, the installation of just about every type of small to medium-size computer system. In the past, these systems operated reliably, with occasional hardware or software "crashes," but few operator-induced mishaps.

Recently, small computers, including personal computers, have become widely used in all environments. Yet, a paradox has developed. Small computer systems are said to have become very reliable, yet these systems seem to fail just as frequently, if not more often, than older computers that were more complex and supposedly less reliable. The reason for this paradox is simple: computers have become highly reliable, but users are now often responsible for the problems.

With older, expensive systems, operators were highly trained in view of the high cost of the system. However, with the more recent computers, operators receive minimal training, if any.

It is true that personal computers have become so simple that anyone can operate them with no prior training, and without any real risk—at least in the beginning. However, if a computer is used for business purposes, suitable precautions must be taken to safeguard information and insure reliable operation.

This book was written to accomplish this purpose. It tells you the DO's and DON'Ts of proper computer utilization. The operative word is generally DON'T; hence the title. Quite simply,

DON'T . . . unless you know what you are doing.

Provided you follow the simple rules presented in this book, you should enjoy years of trouble-free operation.

I would like to acknowledge here the involuntary contributions of the many users of the computer systems I have installed, or have been associated with over the years. Their experiences, as well as my own, have contributed to the body of knowledge and the rules presented in this book.

I would like to express my gratitude to Salley Oberlin and Janet Rampa, who edited this manuscript and contributed many improvements. I would also like to thank Carl Boehme, Ronald Henley, Eric Novikoff, Paul Losness, Dave Haverty, Kathy Du Lude and Erv Slaski, who offered many useful comments.

I would be pleased to hear from all readers regarding any suggestions or improvements they may wish to offer.

Introduction

This book tells you all you need to know to use your computer system simply and safely. It presents the rules and procedures, mostly in the form of DOs and DON'Ts, for each component of the system. The purpose of these DOs and DON'Ts is to insure the integrity of the hardware and the software, as well as the operator's safety and peace of mind. Specific recommendations for each element of the system are covered in the corresponding chapters. Once you understand the reason for each recommendation, you may use a different procedure, or take exception to the rule. However, until then, here is your first rule, a DO:

Follow the rules and procedures strictly.

This book addresses the needs of both the home computer user and the business user. To simplify the use of this book, essential recommendations for the home user are given at the beginning of each relevant chapter. Each important topic is discussed in a separate chapter.

Chapter 1 (Caring For Your Computer) tells you why you should learn and follow proper procedures, and describes typical problems.

Chapter 2 (The Computer System) presents the basic definitions required to understand a computer system. Those readers who are already familiar with these definitions may proceed directly to Chapter 3.

***Chapter 3* (Floppy Disks)** is one of the most important chapters, since diskettes are the most common cause of failure. It explains everything about floppy disks, including proper handling and backing-up, labeling, storage and mailing.

Chapter 4 (Hard Disks) describes the specific requirements of hard disk units.

Chapter 5 (The Computer) explains how the computer unit operates and how reliable operation depends on a proper environment, including clean power lines and protection from electro-magnetic noise.

Chapter 6 (The CRT Terminal) stresses the importance of CRT placement for operator comfort and efficiency.

Chapter 7 (The Printer) explains the problems and precautions relating to printers, with specific emphasis on business-type printers.

Chapter 8 (The Tape Units) discusses cassettes and industry-compatible tapes, and explains the importance of proper handling, rewinding and shipping.

Chapter 9 (The Computer Room) describes the ideal setting for your system—how to plan for it, lay it out, furnish it, provide adequate power, control its environment, protect it against fire, and enforce proper procedures.

Chapter 10 (Software) explains the specific problems and requirements relating to software, including maintenance, procedures and changes.

Chapter 11 (Documentation) stresses the need for complete and effective documentation.

Chapter 12 (Security) helps you protect your system from all ills and mishaps. It tells you how to erect protective barriers, protect valuable business forms, secure the site, hide information, preserve audit trails; it also offers advice on how to protect yourself from computer theft.

Chapter 13 (Help) tells you what to do before you need help and explains where to find it. It also tells you what to do once a problem occurs.

Finally, the appendices offer useful references and addresses.

Many novice computer users prefer to learn through experience. This is a good technique, if you can afford the time and the possible cost. If you would rather learn with a book, read on.

CHAPTER 1
CARING FOR YOUR COMPUTER

Things are always at their best in their beginning.
— Pascal, Provinciales, *4*

INTRODUCTION

The purpose of this chapter is to tell you why you should properly care for your computer and the problems you may experience if you don't. Let us first examine the importance of learning and following the proper procedures.

WHY BOTHER?

Both computer manufacturers and computer vendors will tell you that small computers have become highly reliable and that no one should be afraid to use a system. If indeed the computer is foolproof and there is nothing to fear, then why bother with elaborate care and operating procedures? The answer is that both of these statements have to be carefully qualified. Let us now examine each statement in turn.

ARE COMPUTERS RELIABLE?

It is true that over the years small computers have become highly reliable. This is due to the reduction in the number of required components. The reliability of a computer increases in direct proportion to the reduction in the number of components. It is therefore true that modern computers have become rugged and inexpensive compared to their ancestors. However, the correct statement is that a small computer will operate reliably as long as it is properly cared for. Each component of the computer system has specific requirements that must be followed for reliable operation. These requirements are presented throughout this book.

IS THE COMPUTER FOOLPROOF?

We have stated that most equipment vendors say, "Go ahead and use the computer—there is nothing to fear." This statement is true--there is little to fear—*at least at the beginning* when you have not yet built up a valuable collection of information or programs. However, to be correct, this statement should also be qualified. Once you are using a system "for real," operating on valuable data files, you should exercise due care. A fearless attitude should be moderated by a suitable knowledge of the possible problems that may occur.

If an untrained computer user operates a computer without supervision, damage may be caused to the system. Most frequently, information

will be damaged in some way—typically on a diskette. More rarely, equipment may also be damaged. If the system is used by just one person in a home or office, the damage is likely to have minimal consequences. However, in a business environment where many persons use the same system, a single untrained operator can have a highly damaging effect. In addition, the damage that is inflicted may not be readily visible, as is the case when only part of a diskette is damaged. This problem is called the time bomb effect, and is described later in this chapter. We will now examine two attitudes that are prevalent among first-time computer users.

CONTROLLING YOUR EMOTIONS

Two types of first-time computer users may cause problems: those that have a fear of computers, and those that have a total lack of concern for the system. We will now examine each type in turn.

Persons initially afraid of computers may be discouraged from using a computer because of the necessary precautions that should be taken. As a result, equipment suppliers have always minimized this aspect. However, there is no need to ignore the necessary precautions, nor to be discouraged by them. They are simple and straightforward. In other words, *don't be afraid of using a computer system.*

However, if you are the *manager* or the *owner* of a computer system, you should definitely be afraid of letting an untrained operator use your system in an uncontrolled environment. Always enforce proper training. By providing proper training for the operator, you will dispel any unnecessary fears that the operator may have, as well as protect the system. No damage should be caused as long as basic rules are followed, such as establishing back-up copies of any information that the novice operator will be using.

Generally, if a user is afraid of the computer, remember that this very fear or insecurity may be an asset, as it is generally conducive to learning and following proper instructions. Actually, the other extreme attitude is sometimes a more serious problem: the fearless user.

Many fearless first-time users filled with excitement and blind confidence will promptly, joyfully, and unknowingly, destroy hundreds of hours of work done by others, in their excitement at pressing all of the colored keys. Such behavior should be moderated by the knowledge of all the system malfunctions that can be caused by user neglect or ignorance of the correct procedures.

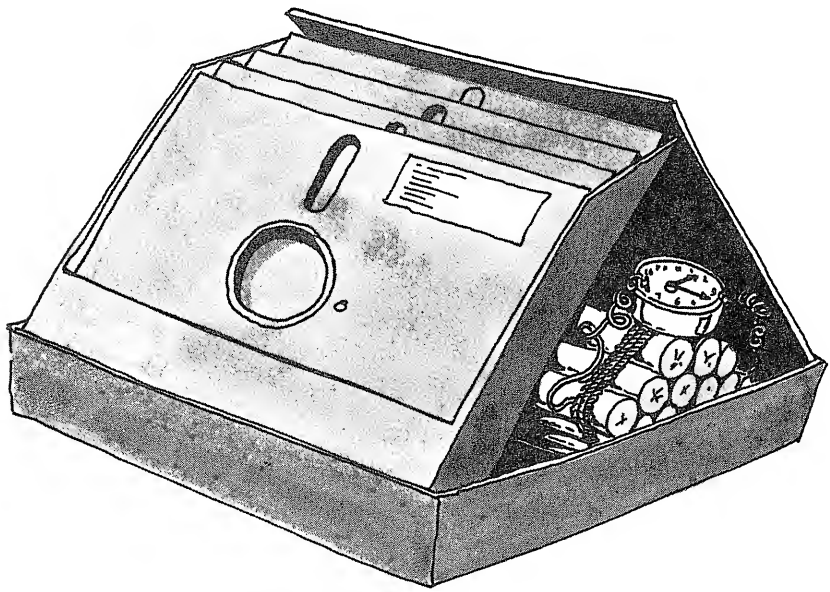
Having stated the need for proper training, let us examine possible problems that may arise. Throughout this book, we will strive to avoid them.

Assuming that the computer system and the programs are operating reliably, the computer user may cause two kinds of problems: permanent damage to a part of the system and temporary disruption to the system. Permanent damage can normally be avoided by using simple precautions. A temporary disruption is usually not serious as long as it does not affect others or destroy any permanent information. However, what appears as a temporary disruption may cause permanent damage. This again is the time bomb effect.

Let us now examine two of the worst situations confronting the computer user: the time bomb effect and the pointed index syndrome.

THE TIME BOMB

Most problems caused by the casual or untrained computer user have no immediate effect. Computer systems are often damaged or endangered in subtle ways that are not easily detectable once the symptoms appear. As a result, failure may occur suddenly and unexpectedly long after the damage was actually done. If the computer system is operated by a single user, who understands how the system works, this person might be able to remember or to recognize the cause of the failure. If the system is used by several persons, however, it may be difficult or impossible to ascertain the cause of the system failure.



The negligent use of a computer system will almost always introduce *time bombs* into that system. As stated, a time bomb is a failure that does not occur until sometime after the original mistake was made. Often, it results in unreliable program operation and damaged files. Many examples will be presented throughout this book. We will stress the proper procedures designed to avoid the time bomb effect. However, in order to insure secure system operation, proper procedures must be enforced *promptly* and *consistently*.

Let us examine the second dreaded situation: the pointed index syndrome.

THE POINTED INDEX SYNDROME

Once a failure occurs, it is often difficult to determine if the failure is due to *hardware* (one of the components) or to *software* (one of the programs or data files). In such a case, the following sequence is unfortunately typical:

- A failure is detected.
- Hardware is suspected.
- The hardware supplier is called in and promptly diagnoses a software failure.
- The software supplier is called and promptly diagnoses a hardware failure.
- At this point, the situation is a stalemate: the hardware person accusingly "points an index finger" at the software person and vice versa. This is the "pointed index syndrome."

Unless a highly competent arbitrator is available, the situation may result in a deadlock because nobody can determine the exact nature of the problem. Unfortunately, this is frequently the case when two separate vendors or maintenance persons are involved. The pointed index syndrome thus compounds the time bomb effect: not only is a proper diagnosis difficult, but no obvious clue appears, and the cause of the failure may have been long forgotten. Today, with reliable microcomputers, the problem often lies with an untrained operator who has unwittingly set up booby traps throughout the system, thus creating chaos.

These problems should not be dismissed lightly. Many systems may operate or appear to operate well for a long period of time until the time bomb

effect takes place and the system suddenly fails. For example, let's consider a situation where new data have been entered onto a disk and gradually built-up over a period of months. Unknowingly, an untrained operator has damaged the disk. But, in this case, it is not until the disk is nearly full that the failure is detected. By that time, the entire file—the result of months of effort—is affected and may not be salvageable. Further, the malfunction might be attributed to faulty hardware or software when it is, in fact, due to the operator. The problems we have just pointed out are serious, but easy to avoid.

IT IS SO SIMPLE

In summary, modern computer systems are simple and easy to take care of. However, they do require a highly disciplined approach. It is therefore important to understand the proper handling of each element of the computer system as well as the proper overall procedures that must be followed. Observance of the rules that are presented in this book should eliminate most operator-caused malfunctions and thus result in a high level of reliability.

CHAPTER 2
THE COMPUTER SYSTEM

You have to study a great deal to know a little.
— Montesquieu, Pensees

INTRODUCTION

This chapter presents the basic definitions necessary to understand the elements and operation of a complete computer system, including hardware, software and peripherals. We will first describe the main logical elements of the system, then we will define those terms relating to the monitor, the memory, the operating system, the files, the mass storage media, the CRT terminal, and the printer.

A *computer* is an electronic device that executes a *program* and communicates with the outside world via peripherals. The programs executed by the computer create or manipulate *data*. Examples of data are numbers and text. Both programs and data are normally stored as *files* on *magnetic storage devices,* such as cassettes, tapes or disks. A file is a collection of information that has a name and can be manipulated as a unit.

In order to execute a program, the program must first be transferred from the disk or cassette to the *memory* of the computer. This is called *loading* the program (see Figure 2.1).

The program is then executed by the *central processing unit* (CPU), and will usually cause input and output operations to occur. Information is obtained from an *input device,* such as a keyboard, and transmitted to an *output device,* such as a CRT (Cathode Ray Tube) display or a printer. The *input/output* section of the computer manages such transfers of information. By supplying information or commands via the input device and receiving information via the output device, the operator can carry on a dialogue with the program. Generally, the operator types at the keyboard while looking at the screen of a CRT terminal. A *CRT terminal* is a standard *peripheral* that includes a keyboard and a television-like display.

A simplified model of a computer system is shown in Figure 2.2. The *computer system* includes the computer proper plus peripheral devices for input, output and mass storage. The *computer proper* is indicated by a dashed line. It includes three functional modules: the memory, the CPU, and the input/output. The packaging of these three modules varies, but each module is always included. For example, business computers often package the memory, the CPU, and the disk units in a single enclosure, while home computers often incorporate the memory, the CPU and the keyboard in a single enclosure.

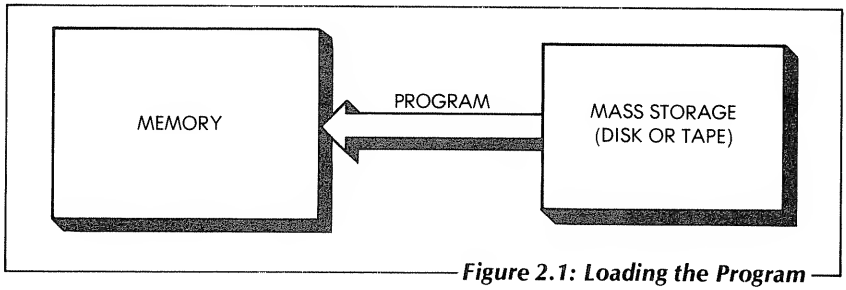


Figure 2.1: Loading the Program

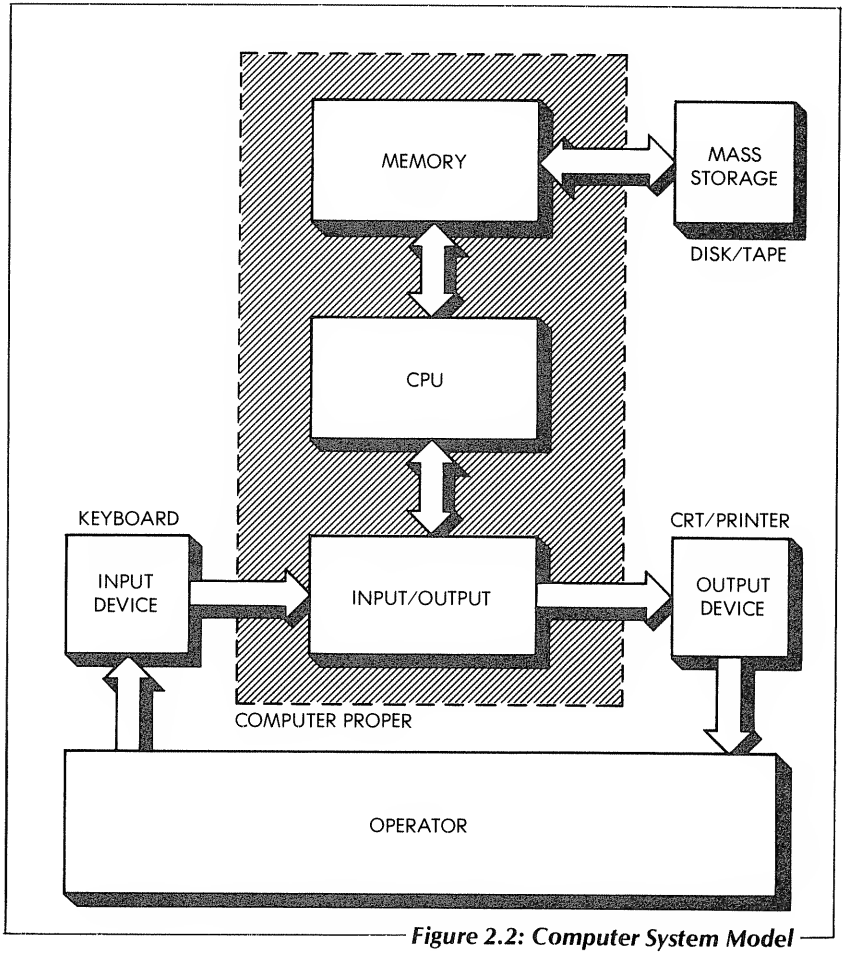


Figure 2.2: Computer System Model

THE MONITOR

In addition to the necessary hardware elements, suitable *software* (i.e., the programs) is required to operate a computer system.

At a minimum, a program called the *monitor* must be present when a computer is first turned on. Unless a permanent portion of the computer's memory contains such a monitor program or a *bootstrap* program that loads the monitor, nothing will happen when it is turned on. All commands typed at the keyboard will be ignored by the hardware. The role of the monitor program is to collect the characters typed on the keyboard and to interpret them as commands as they are typed. The monitor is a program that monitors the keyboard and carries out the minimal set of actions required to operate the system (i.e., displaying text on the screen, typing text on the printer or loading programs from disk or tape). A monitor is often permanently installed in the computer system and is generally stored in *ROM* (Read Only Memory), a non-volatile form of memory inside the computer proper. Each computer system is normally delivered with a monitor. Thus, when the computer is turned on and an appropriate command is typed at the keyboard, the command is recognized and executed. Often, this command will cause a suitable program to be loaded, under the control of the monitor, from a mass storage device into the computer's memory.

THE MEMORY

There are two types of memory inside the computer: ROM and RAM. While the contents of *ROM* (Read Only Memory) are fixed and never disappear, the contents of *RAM* (Random Access Memory) may be read or written and thus may be changed at will.

Unfortunately, at the present state of technology, RAM memory is volatile and will not retain its contents once power is no longer applied. This means that when the power is turned off, any program or data that may have been stored inside the computer's memory is lost except for the permanent monitor or bootstrap that is stored in ROM.

In the case of home computers, as well as in the case of industrial control computers, programs that are most frequently used are permanently stored in ROM in the computer's memory. The advantage of storing them in ROM is that they are no longer volatile and do not need to be reloaded from the mass storage device each time the power is turned off and on. For example, most low-cost personal computers provide a built-in BASIC interpreter in ROM, which makes it possible to type in instructions directly in BASIC (a programming language). However, the total amount of ROM

and RAM memory is limited. Storing a program like a BASIC interpreter in ROM decreases the amount of RAM memory available for executing other programs. Business or scientific computers are therefore designed with a small ROM memory, and a large RAM memory, since many different programs must be used.

Typically, microcomputers are limited to a maximum memory size of 64K bytes (1K represents 1,024 or 2^{10}). A *byte* is a group of 8 bits used to represent a character or a digit in binary form. A *bit* is a binary digit (0 or 1). All information inside the computer is stored as groups of bits. A simple monitor may require 2K bytes of ROM. A good BASIC interpreter may require 16K of memory, either ROM or RAM. If the BASIC interpreter is stored permanently along with the monitor in ROM, the total amount of ROM becomes 18K, thus restricting the maximum amount of RAM that may be added to the system to 46K (64K minus 18K). This restriction is not acceptable in general-purpose business systems. With these systems, the computer's ROM contains only a small program, either a minimal operating system or a bootstrap, which is necessary to load the monitor or the operating system from disk or tape into RAM. This way, a large amount of RAM is available for the various programs run at different times on the business computer.

THE OPERATING SYSTEM

The *operating system* provides all of the facilities required to use the peripherals, to load other programs, and to communicate with the system. A monitor is a simple operating system. More elaborate facilities are required in order to use a disk-equipped system conveniently. For example, it must be possible to load program or data files by name. Thus, typing:

```
WORDPROCESSOR
```

or

```
BASIC
```

will automatically activate the corresponding program. The operating system will first load the program from the disk into the computer's memory, and then it will activate it.

Similarly, it must be possible to copy files or entire diskettes, to change names of files, to interrupt the execution of a program, and to set various typing options. All of these functions entail the interpretation and proper execution of commands typed by the user. This is the function of the operating system program.

The operating system provides all the facilities required for convenient system operation. A good operating system makes most of the hardware details of the computer system transparent to the user. In other words, the user may use symbolic names for programs and files and manipulate them without being concerned with details, such as their exact size or their location in memory or on disk.

A good operating system also provides a number of *utilities,* which are programs designed to facilitate specific aspects of data processing. For example, an *editor* program is usually provided in order to conveniently type in and modify text on the screen. Other specialized programs may be provided to display programs or text, or to print them in an attractive or convenient format. Still other programs may be supplied to perform specialized transfers such as copying diskettes or files from one medium to another. There are many proprietary operating systems available. An example of a widely-used operating system for 8-bit microcomputers is CP/M.

THE FILES

Recall that a file is a collection of information that resides on a mass storage device such as a disk or a tape. Either programs or data (such as text or numbers to be manipulated by programs) may be stored permanently as files. Each file is given a name. As mentioned before, one of the primary purposes of the operating system is to make file-handling invisible to the user. In addition, sophisticated operating systems allow files to have *attributes,* such as a list of authorized users, or protection features such as specifying a file type as read-only, in which case the file may no longer be modified.

Two types of files should be distinguished: *system files* and *user files.* System files contain those programs that are indispensable for using the system, such as the operating system itself, and any language interpreters, such as BASIC or Pascal. User files contain those programs and text or data that belong to the user. Typically, system files are stored on a mass storage medium (disk or tape) that is accessible to all users. On the other hand, private user files are typically stored on a removable storage medium that can be retained by the user. Naturally, in some systems it is not practical to physically separate system files from user files. Therefore, both types of files reside on the same medium. This is often the case, for example, with large fixed-head disks.

Files hold information and programs. Like the equipment, they are very valuable and must be protected. Most procedures and recommendations

presented in this book are aimed at protecting the files as much as the hardware.

THE MASS STORAGE MEDIA

ROM and RAM provide the computer with a fast-working memory required for fast CPU operation. When not in use, files are stored on less expensive *mass storage media*. There are two main types of mass storage media: disks and tapes.

Disk Units

A *disk unit* includes a drive mechanism and a disk that stores information on its surface, just like a magnetic tape. Two types of disks are used: *floppy disks* and *hard disks*.

Floppy disks or *diskettes* are a low-cost storage medium. Floppy disk drives are generally used in pairs (so that the contents of one disk can be easily copied to another). Programs or data may be recorded on one side of a *single-sided* diskette or on both sides of a *two-sided* diskette. In addition, a *double-density* format is often used to achieve a higher storage capability per disk.

The standard size floppy disk is 8 inches in diameter. The smaller floppy disk, generally called a *mini-floppy* or *minidiskette,* is 5-1/4 inches in diameter. Each type of diskette requires a specific type of disk drive. This will be explained in Chapter 3.

Because of their low unit cost, floppy disks are the most prevalent storage device for small computer systems. However, their storage capacity is too small and their access speed is too slow for larger business applications. For such applications, hard disks are used.

A hard disk is generally 8 to 14 inches in diameter and like a floppy disk, it stores information on either one or both sides (see Figure 2.3). Because of its rigid construction, a hard disk can be equipped with a more precise access mechanism than a floppy disk. This allows it to store much more information and to have a faster access speed. There are several types of hard disks. For example, in order to increase their storage capacity, hard disks are often combined in stacks of several disk platters. Also, removable cartridges are used to facilitate operator handling, to make backup copies and to transfer information to another computer.

Floppies and hard disks require different operating procedures. The handling of disks is the area where most problems occur. Therefore, detailed procedures for handling both types of disks will be presented in Chapters 3 and 4.

Tape Units

Two main types of tape units are used with small computers: *cassettes* and regular *tape drives* (generally IBM compatible).

Cassette tapes are the most economical type of mass storage device but they suffer many drawbacks. They are slow, sometimes unreliable, and provide limited storage capability. They are normally used for small files and as a minimum-cost storage device on the least expensive systems. They are sometimes incorporated in a terminal as a convenient way to load and unload information.

Regular tape drives are relatively fast and can store a very large quantity of information. However, unlike a disk, once data is stored on the tape, it must be retrieved *sequentially*. It is not possible to change a record of data at a random location on the tape. As a result, tape units are generally used only as a backup for a hard disk, and not as the main storage device.

THE CRT TERMINAL

The *CRT terminal* or *Video Display Unit* (VDU) is equipped with a television-like tube or CRT (Cathode Ray Tube) on which characters or graphics are displayed. A typical business CRT is shown in Figure 2.4. Normally, the screen measures 12 inches diagonally and can display 24 lines

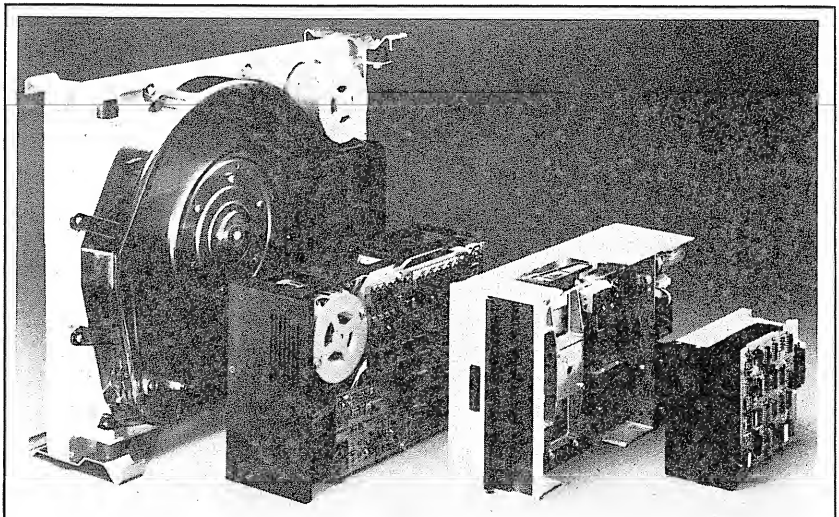


Figure 2.3: Hard (Left) and Floppy (Right) Disk Drives

of 80 characters, in both upper and lower case letters. The *keyboard* has keys analogous to a typewriter's, plus additional *function* or *control* keys, and often a separate *numeric keypad* with the digits 0 through 9.

The CRT terminal is the primary means of communicating with a personal or business system. The keyboard on a CRT is the usual input medium for the computer. The keyboard and the screen can be separate units connected to each other with an interconnection cable, or they may be indirectly connected to each other through the computer, as shown in Figure 2.2. In this illustration the keyboard is connected to the *input* portion of the computer, and the CRT screen is connected to the *output* portion of the computer. Thus, a character typed on the keyboard is normally echoed *via the computer* onto the screen.

Whenever the computer proper integrates the keyboard as a part of the cabinet, it is not necessary to use a full CRT terminal as an output device. An ordinary television set or a *video monitor,* i.e., a screen, can be used for that purpose.

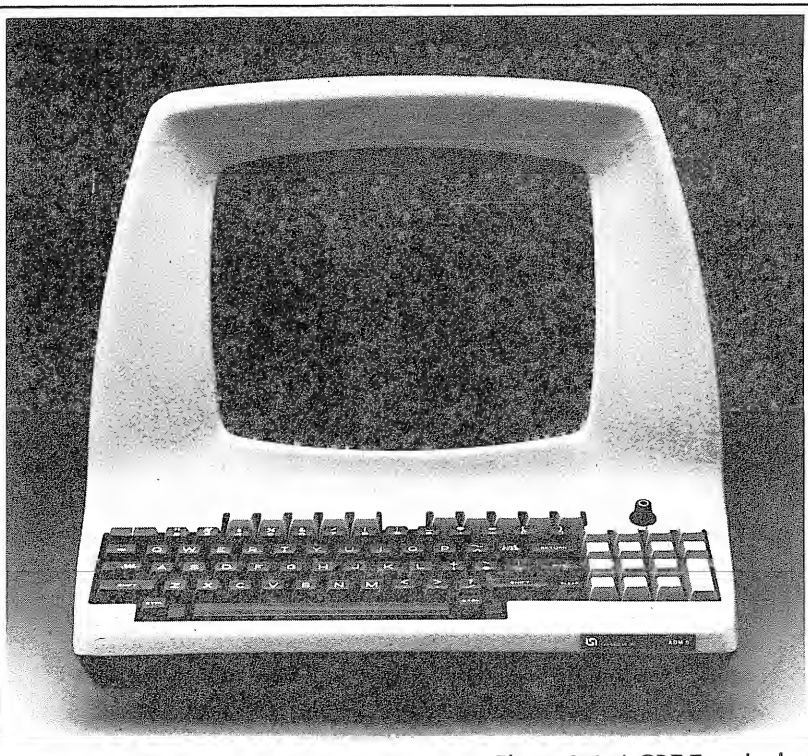


Figure 2.4: A CRT Terminal

THE PRINTER

A *printer* is indispensable for business applications since the CRT does not provide a hardcopy of the information that it displays. The printer is the only device that can record easily readable information permanently. It has the largest number of mechanical components and can be the most expensive piece of hardware in the system. It also has the potential to be the least reliable.

SUMMARY

We have introduced the basic elements of a computer system, from hardware to software, including important concepts such as files. Next, we will examine each of the modules and present specific recommendations. We will first discuss the floppy disk, as this is the number one problem area.

CHAPTER 3
FLOPPY DISKS

Out, damned spot! Out, I say.
— Macbeth V

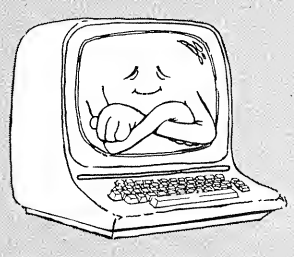
FOR THE HOME COMPUTER USER

The main rule is:

Back-up each important diskette before using it.

Other important rules are:

- Respect the physical and magnetic integrity of the diskette: Don't touch its exposed surface. Don't fold it or compress it. Don't place diskettes near magnetic coils or magnetized objects.
- Label the diskette promptly. Don't use a hard-tipped pen.
- Maintain the proper environment: Avoid heat and dust.
- Read this entire chapter. It is the most important one for you if you use diskettes.

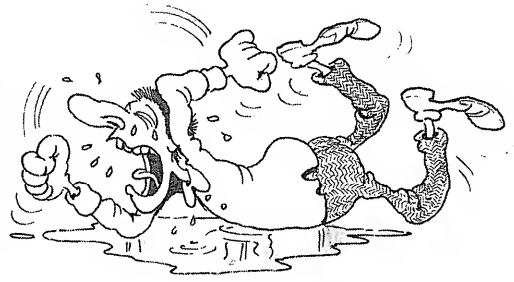


INTRODUCTION

Floppy disks are probably the main cause of failures in any computer system that uses them. Nearly all such failures are caused by user mishandling. These failures can be prevented by respecting the rules presented in this chapter. A careful reading and understanding of the information presented in this chapter will probably eliminate 75% of the failures that are apt to happen on a computer system with floppy disks.

Failures due to diskette mishandling usually have tragic consequences. They can destroy crucial data or cause strange symptoms that are hard to diagnose.

Here is a typical horror story.



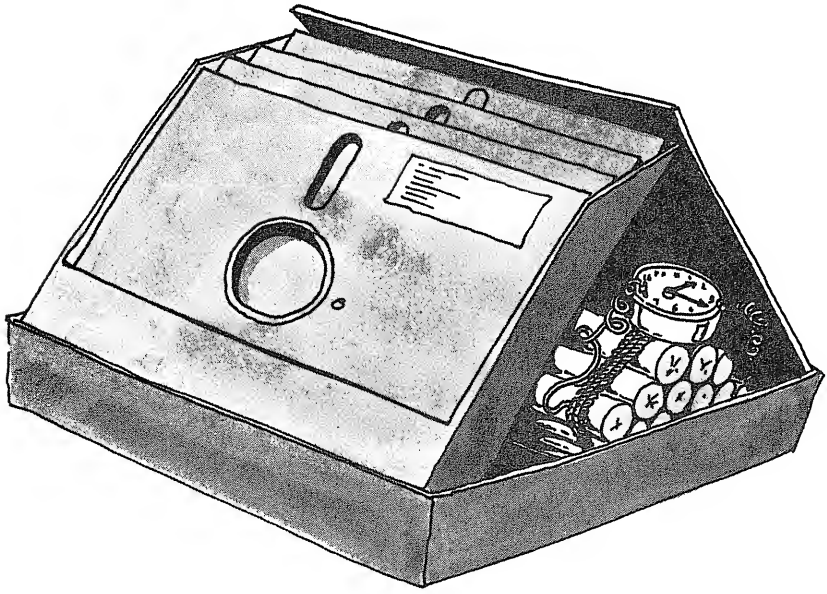
In order to start Computer System A, a diskette is inserted into one of the disk drives, and a command is typed at the terminal. Normally, the effect of this command is to load the contents of a program from the diskette into the computer's memory.

Unfortunately, one morning, the computer system, which was operating perfectly up to this time, began to resist all attempts to load from the diskette. As a result, no work could be done on the computer. The maintenance person was called in, showed up the next day, took the computer apart, reassembled it, and mumbled something about a bad contact in the XYZ unit. The computer began operating again.

A few weeks later, a new problem occurred; this time, the computer started properly. However, the data file containing all the customer names could no longer be read. After replacing a few boards inside the computer, all in vain, the maintenance man concluded that the software was bad. In this "fortunate" case, the company that provided the software determined that the software was good and suspected the diskette that held the customer names. After much debate between the hardware supplier and the software vendor, the conclusion was drawn that both the hardware and the software appeared to be working, but the data file was bad.

To make a long story short, one of the computer operators had

used a ball-point pen to label the diskettes. In doing so, the operator damaged the contents of the diskettes by applying pressure against their cardboard jackets. With the pressure of a pen, dust present inside a jacket is imbedded on the diskette, thus damaging it. The first time the pen was used, the main system diskette used to store the operating system was damaged. The second time, an essential data diskette was damaged. Unfortunately, the damage that had occurred to the data diskette was not immediately detected, and the offending operator was not around when the system failed. Easy diagnosis was no longer possible.



This story illustrates the "time bomb" effect that can occur when operators mishandle the equipment. The problem could have been easily prevented had the operator been trained in proper diskette handling. The hardware and software both operated correctly; the problem occurred because of an inadequately trained operator who damaged several diskettes in an almost unnoticeable way.

To avoid the "time bomb" effect, proper discipline must be used and enforced for the handling of diskettes. Remember that most actions that damage a diskette do not damage it in a way that is immediately visible. For example, contamination by dust or physical damage may not be detected until days or even months later when the affected area of the

diskette is read by the disk drive. At that point, the computer might be fooled by incorrect information on the diskette and, consequently, irreparably damage the entire contents.

Once you understand the proper precautions that must be used when handling a diskette, you can avoid many problems by simply using common sense. In this chapter we will first explain what a diskette is and how it is used; then we will present step-by-step recommendations and rules for handling and using a diskette properly, including labeling, storing, mailing, and traveling with diskettes. Environmental constraints, maintenance procedures and common failures will also be described. First, let us examine what a diskette is, and how it works.

UNDERSTANDING YOUR DISKETTE

We will now present the main definitions relating to diskettes, examine the main techniques used for recording data, and discuss the techniques for retrieving the information that was recorded. We will then proceed to the proper handling of a diskette. Let us examine first the diskette itself, then its jacket.

The diskette is flexible and constructed of mylar material, coated with a magnetic oxide. It is enclosed in a square jacket, and rotates inside the jacket when being accessed. The jacket is lined on the inside with a special low friction material that automatically cleans the diskette by trapping dust particles. Data is recorded on the magnetic coating of the diskette.

Diskette Types

Diskettes come in many varieties, and each type requires a specific disk drive. There are four major differences: size, number of sides, recording density, and sectoring technique. Let us examine these terms.

Diskettes come in two standard sizes: 8 inch and 5-1/4 inch. The 8-inch diskette is called a *floppy* disk, a flexible disk or a diskette. The 5-1/4 inch diskette is called a *mini-floppy,* or a minidiskette. The two sizes of diskettes are shown in Figure 3.1.

Diskettes may also be *single-sided* or *dual-sided*. Generally, only one side of the diskette is used to record data and the diskette is called single-sided. Sometimes, however, both sides are used to record data and this type of diskette is called dual-sided. Single-sided diskettes look the same as dual-sided diskettes. If you use both kinds, identify them carefully.

Data may be recorded on the diskette in either *single-density* or *double-density* format. Double (or dual) density allows the storing of more data,

but not as reliably as single-density format. Again, double-density diskettes look just like single-density ones. Label your diskettes accordingly if you use both types of drives.

Finally, diskettes may be *soft-sectored* or *hard-sectored*. Information on the disk is organized in *tracks* and *sectors*. In order for the disk drive to detect the beginning of the first sector, an *index hole* is punched in the disk. Two different techniques are used for indicating the beginning of the other disk sectors: *soft sectoring,* and *hard sectoring.*

In the soft sectoring technique, the disk has only one index hole marking the beginning of the first sector. The drive then computes the location and position of each subsequent sector. An identification number is written on the disk at the beginning of each sector for positive identification.

In the hard sectoring technique, a hole is punched on a special track of the disk for each sector position. Several hard sectored formats are used, such as 10, 16 and 32 sectors, depending on the manufacturer and the software requirements. Soft and hard sectored disks are physically different and can easily be distinguished by the number of holes.

We have described four types of diskettes. Remember that your disk drive normally accepts only one type of diskette, and no other. For example, it may require an 8'' single-sided, single-density, soft-sectored diskette.

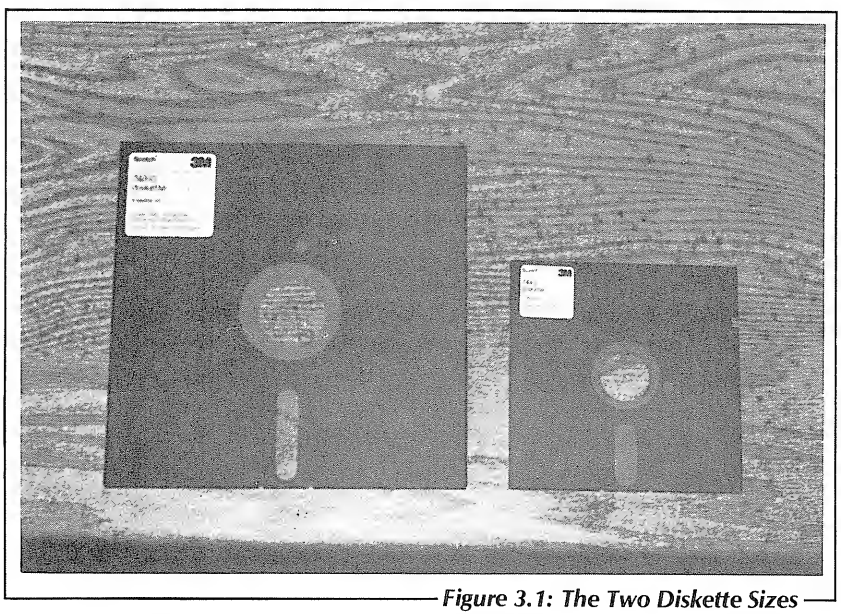


Figure 3.1: The Two Diskette Sizes

Don't mix types. When purchasing additional diskettes, you must know which type of diskette is required.

Before we explain the function of the various openings in the jacket, let us examine how data is recorded on the diskette.

Data Recording

Data is recorded on the disk in binary format as sequences of 0s and 1s (bits), and stored as magnetic patterns along concentric circles called *tracks*. A regular 8 inch diskette generally has 77 tracks, while a 5-1/4 inch minidiskette can have 35, 40 or 77 tracks per surface. As shown in Figure 3.2, information is structured in *sectors* along the tracks. A whole sector is always read or written at a time, and all data on the disk is identified by a sector number and a track number. Each track can be accessed by moving the head of the disk drive along a radius of the disk.

A mechanism must be provided so that the disk drive may identify any given sector on any track. We have already seen that one of two techniques may be used for this purpose: hard sectoring and soft sectoring.

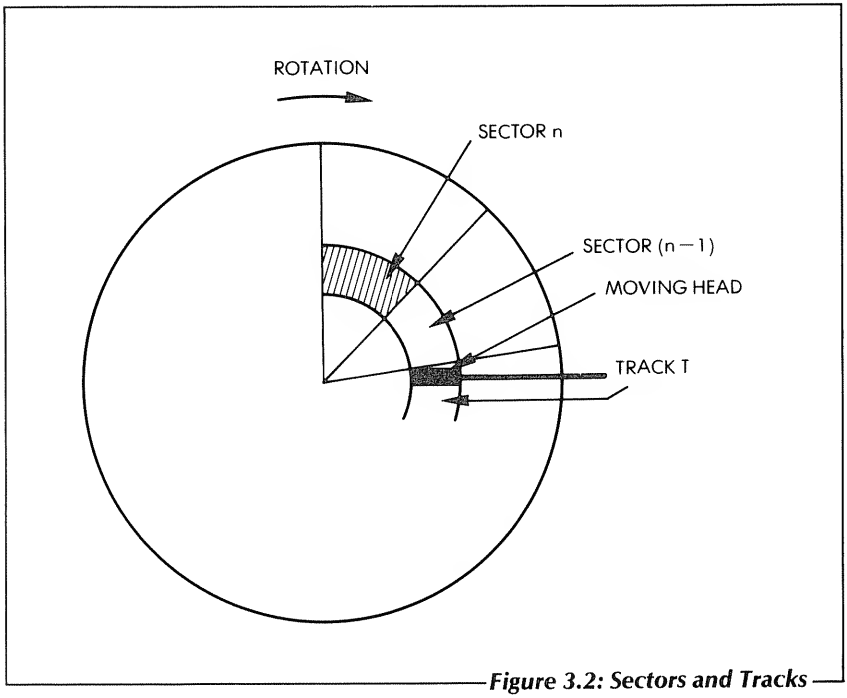


Figure 3.2: Sectors and Tracks

The read/write head of the disk drive operates like the head of a tape-recorder. The head is applied against the disk surface, while a felt pressure pad is applied against the other side. Any defects in the disk surface, such as dirt or creases, will thus cause loss of information.

When a disk drive is misadjusted, or when the head is dirty, the surface of the diskette is generally damaged, resulting in shiny rings on the surface of the diskette. Inspect your diskettes regularly for such clues.

We have already seen that data may be recorded in one of two formats. Data may be recorded at the surface of the disk either in a single-density format (3,408 bits per inch or bpi) or in a double-density format (6,816 bpi).

The jacket containing the diskette has several roles: protecting the diskette, allowing access to the drive motor and to the drive sensors. These roles are accomplished by the special jacket liner already described and by specialized openings. These openings will now be described.

The Jacket

The jacket has several openings. The center hole or *disk hub* allows the spindle of the disk drive motor to grasp and rotate the diskette inside the jacket at high speed. A diskette should be replaced when the edge of the hole is cracked or torn.

The *access slot* in the jacket (shown in Figure 3.3) allows the read-write head of the disk drive to come in contact with the diskette and to read or write information on the surface of the disk (see Figure 3.4).

The *index hole* on the diskette marks the position of the first sector. A sensor in the drive detects the index hole as it passes by the corresponding jacket hole (see Figure 3.3). Recall that a hard sectored disk has maybe 20 or 32 sector holes in addition to the index hole. A soft sectored disk has only one index hole. The hole is normally on the inside of the disk, except for Memorex disks, where the outer part of the disk is used.

The *write protect* or *write enable* notch is optional. This notch may be used to prevent accidental writing of information on the disk. A write protect or write enable notch allows the user to protect valuable programs or data from inadvertent writing. With an 8-inch floppy, the diskette is write-protected when the notch is exposed, i.e., no information may then be written on the disk. If the notch is covered with a small aluminized square, data may be freely written on the disk. In the case of a mini-floppy, this convention is reversed. Information on the disk is protected when the notch is covered; otherwise, it is not protected. Diskettes are sold either with or without a protection notch. This feature must be specified at the time of purchase.

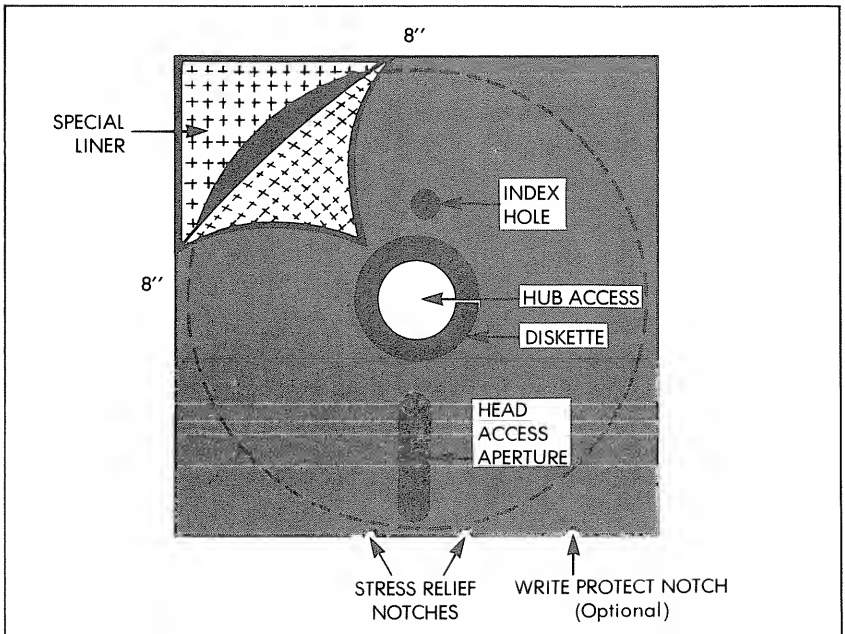


Figure 3.3: Details of a Diskette

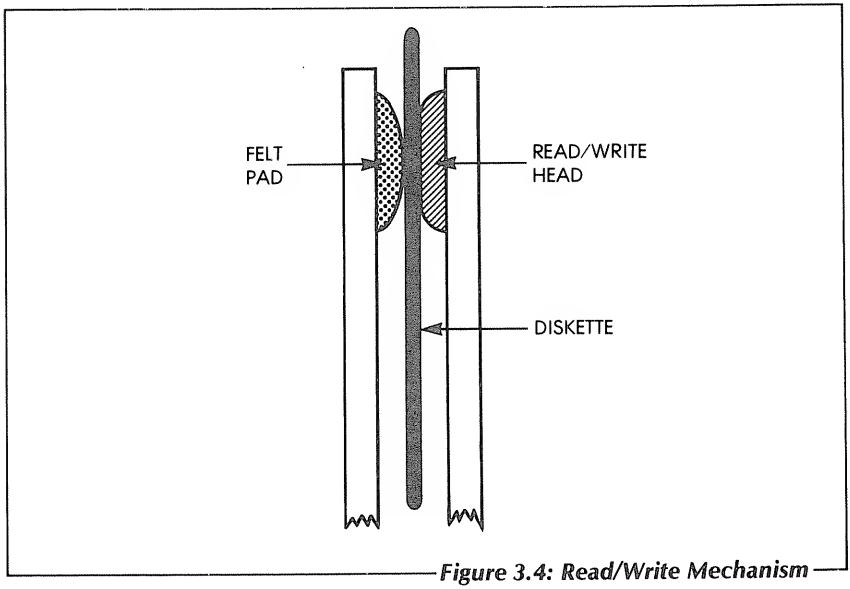
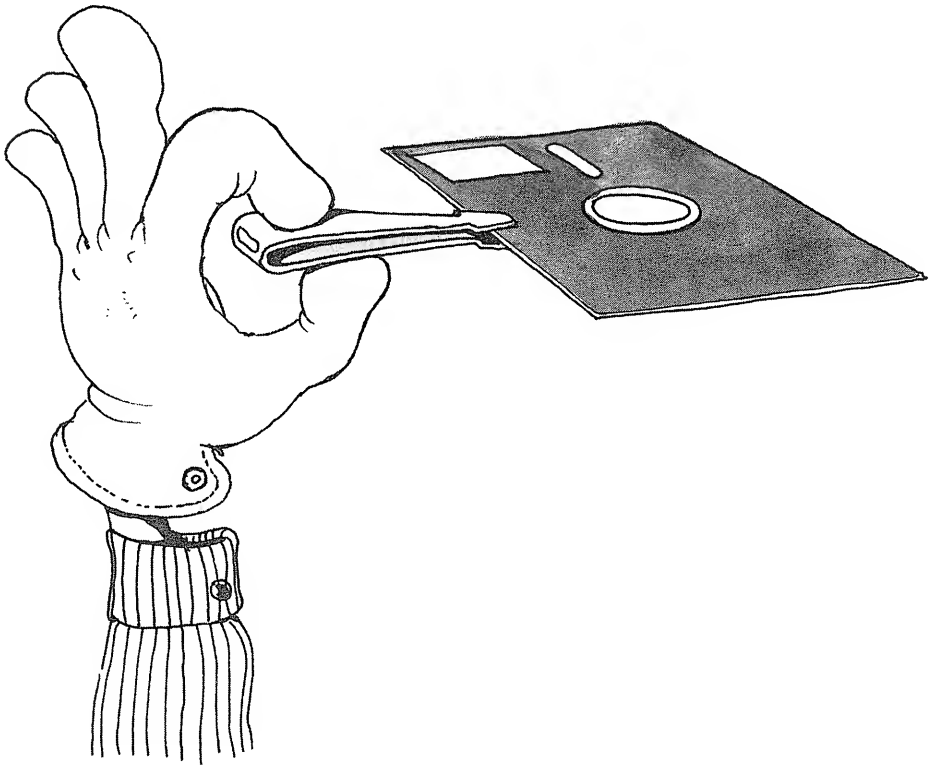


Figure 3.4: Read/Write Mechanism

Alignment/strain relief notches are used to position the diskette correctly. They normally face towards the rear of the disk unit.

Having learned the various types of diskettes, how data is recorded, and the purpose of the various openings in the jacket, let us now learn how to handle a diskette properly.



HANDLING THE DISKETTE

Proper diskette handling is essential to the reliable operation of your system. Improper diskette handling probably causes most "computer problems." Improper handling "pollutes" the diskette by damaging a few bits (or more) of information. The damage may only be detected much later, thus causing the time-bomb effect for the same user or a subsequent one.

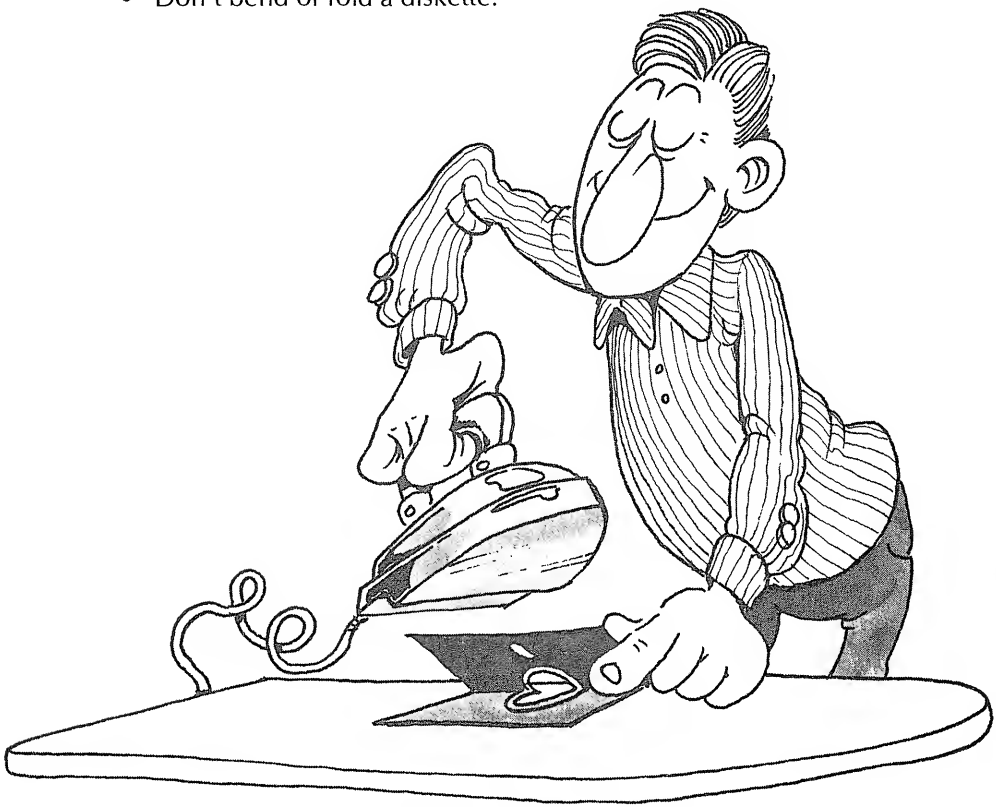
Once you understand the nature of your diskette and are aware of the main dangers, proper diskette handling is quite simple. Most importantly, you must respect the physical and magnetic integrity of your diskette.

Remember the four main characteristics of a diskette:

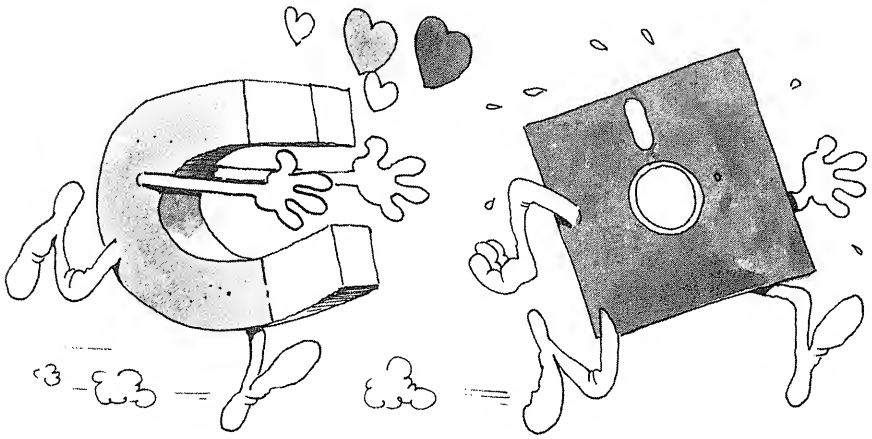
- It is fragile.
- The data is recorded on a magnetic surface, which is sensitive to electromagnetic fields.
- The magnetic surface is exposed to the environment through the openings in the jacket.
- There is only one correct way to insert a diskette.

Let us examine the rules resulting from these characteristics:

- Respect the physical integrity of a diskette.
- Don't bend or fold a diskette.

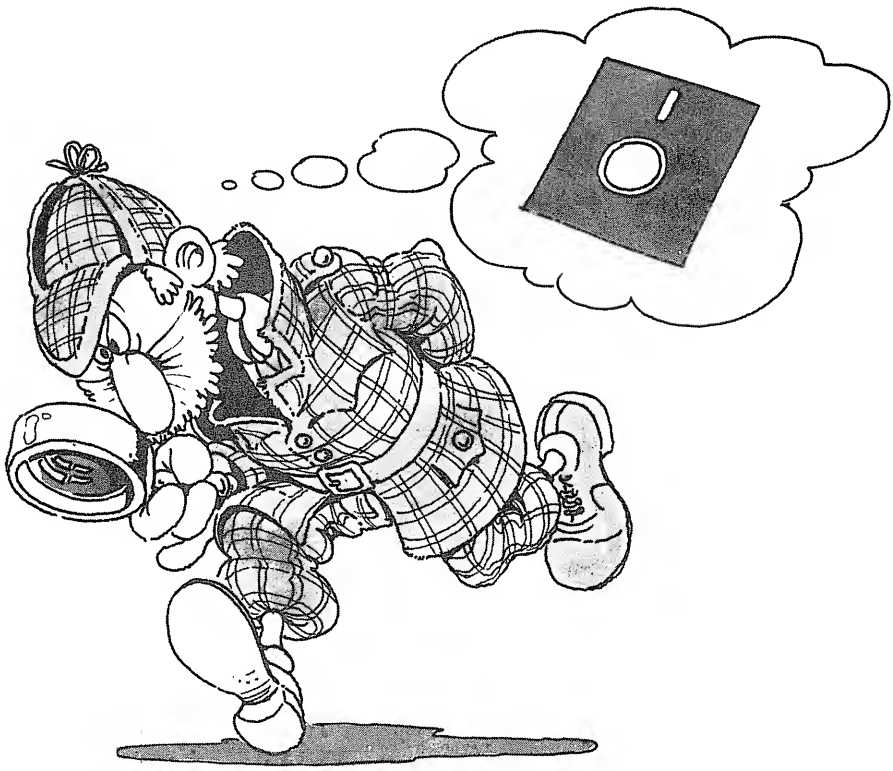


- Don't touch the surface of a diskette. The oily chemicals secreted by the skin of your fingers will permanently damage an area of a diskette.
- Keep all sources of magnetic fields away from diskettes, including magnets as well as magnetized objects.



- Maintain the proper working environment. Avoid heat, moisture and dust.
- Insert the diskette into the drive properly.

It is unfortunate that many computer users do not believe in taking strict precautions because they see no immediate ill effects. Because damage generally occurs to only a very small area of the diskette, the diskette might be used for a long time with no visible effect. It is only when data is read or written to or from the damaged area that strange problems start to occur. Because the data stored at the damaged area is modified, the system might start behaving in a strange way that is not directly traceable to a bad diskette. Hence, the strange behavior may be attributed to bad hardware or software, thereby eluding easy detection. It is therefore imperative to insist on proper diskette handling by *all* users.



Now that we know how to handle a diskette properly, we are ready to use it.

USING THE DISKETTE

When using a diskette, four essential recommendations apply:

1. Protect each new diskette.
2. Insert the diskette correctly.
3. Follow a proper power-up/power-down procedure.
4. Inspect diskettes each time they are used.

Let us examine these recommendations.

Protect Each New Diskette

Each diskette is normally contained in a paper envelope (see Figure 3.1). When you first receive a diskette, immediately inspect the envelope for signs of obvious damage. Remove the diskette from the envelope and

inspect it for damage. A diskette that has been physically damaged should be presumed to be bad and must be rejected. Don't touch the magnetic surface of a diskette with your fingers or any sharp object.

Remember: if the diskette contains a new program that you have just received, your first reflex should be to make a copy of the diskette and to file the original away in a safe location. Work with the copy that you have created. No exceptions. No excuses.

If you ever wipe out the only copy of a new program that you have just received, you will be convinced that this recommendation is correct. Unfortunately, by that time, it will be too late. This is one area where bitter experience should not be required.

If you are not yet familiar with diskettes, set the write-protect mode on your diskette, by either peeling off or sticking on the aluminum square on the notch (depending on diskette size), if your diskette has this feature. Use a blank diskette for writing information rather than the one that contains the program. Using the write-protect mode will prevent erroneous writing or erasure of information on your program diskette—provided you insert it correctly.

Now insert the diskette by applying the "rule of thumb."

Insert The Diskette Correctly

Hold the diskette in your right hand between your thumb and index finger, placing your thumb on top of the square diskette label. Open the door of your disk drive and insert the diskette, slowly and firmly until you hear a "click." Then close the door of your drive (if it has one). In most cases, disk drives are designed so that you will correctly insert the diskette automatically if you follow the "rule of thumb," i.e., if, when you hold it, your thumb is pressing against the diskette's label.

When a disk drive is mounted vertically, it is usually on the right side of the screen or the computer, and the diskette label usually faces to the left. When the disk drive is mounted horizontally, the diskette label normally faces up. The longitudinal head access slot is normally inserted first, in the direction of the drive (see Figure 3.5).

If you insert the diskette the wrong way, damage to the data stored on the diskette may result.

There are eight different ways to insert a diskette, but there is only one correct way. Any other way might damage it. If unskilled operators will be using your diskettes, it may be a good idea to print labels that display a large arrow and to place an arrow on each disk jacket indicating the proper way to insert the diskette. This will help to reduce errors when the diskette is inserted into the disk drive.

To remove the diskette, open the door of the disk drive, pull the diskette out, and put it back into its envelope immediately. Then, place the diskette on a horizontal surface *away from the computer* or other electromagnetic equipment or put it in its proper holder or container. (These holders will be described later in this chapter.)

Power-Up/Power-Down

As a general rule, never insert a diskette into a disk drive until power to the entire computer system has been turned on. If the computer can be turned on separately from the disk drive, it might accidentally write random data on the diskette. In systems where the disk drive is powered directly from the main computer, a diskette may generally be inserted in the disk drive before the system is powered up. If in doubt, don't insert a diskette until power has been turned on.

Conversely, always remove the diskette prior to turning the system off. If the system is turned off while the diskette is still in the disk drive, random

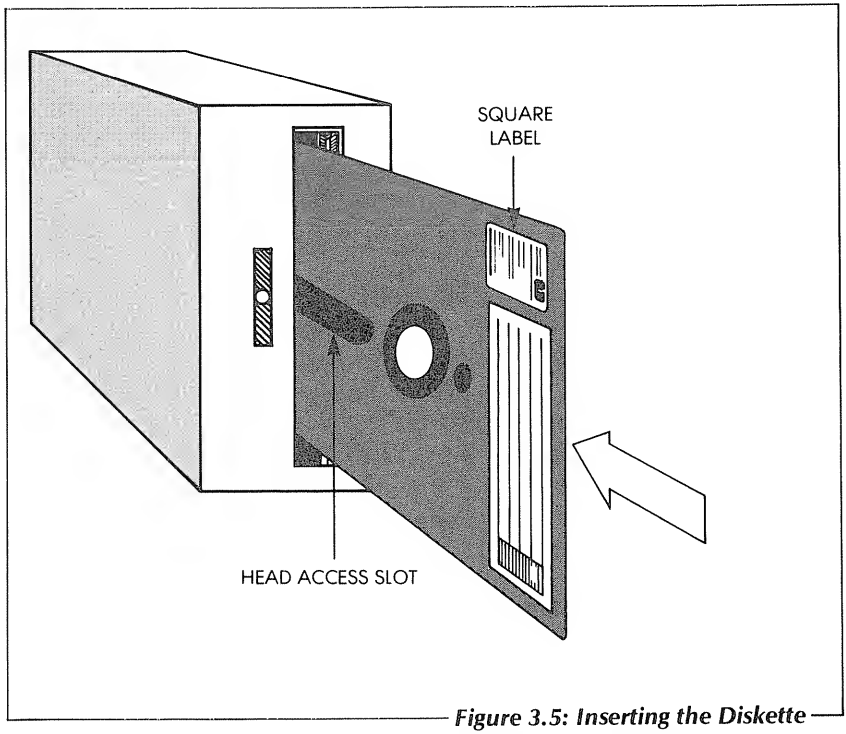


Figure 3.5: Inserting the Diskette

data might accidentally be written onto the diskette, thus wiping out some of its contents.

Inspect Your Diskette

Periodically inspect the round hole at the center of the diskette. This hole contacts with the hub that presses on the diskette and rotates it at high speed inside its jacket. Over time, this hole will deteriorate. Most of the damage occurs because of improper insertion. Most microcomputer disk drives simultaneously apply the read/write head and the hub to the diskette so that the diskette positions itself with the hub already through the hole. As a result indentations may appear. Once this hole is damaged, the diskette should be replaced.

Also, examine the surface of the diskette that is visible through the head access hole. Over time, shiny rings will appear. However, scratches, folds, or very shiny wide rings indicate trouble. When these signs appear, test your diskette with a special program, or simply discard it.

BACKING-UP

One of the most important defensive measures when using diskettes is to frequently make a backup copy of the information stored on the diskette. Always assume that at some point the data contained on the diskette will be damaged, either by yourself or by someone else. Therefore, as soon as any significant change is made on the diskette, a copy should be created and stored at a safe location.

When backing-up a diskette, it is recommended that you store the copy at a different location than the location where the original is being stored. The reason for this is quite simple. An undisciplined user is likely to pollute the original diskette and then to pollute the backup diskette if it is readily accessible. To guarantee a reliable backup, the duplicates should be stored far away from the original that they intend to protect. Don't hesitate to create multiple backups but make sure that they are all properly labeled. Always write the date when the copy was made on the label of the backup diskette. (Remember: Use a soft-tip felt pen only—don't use a ball-point pen or a pencil.)

We have now learned how a diskette looks, how it works, how to handle it, and how to insert it. There is still more to learn: how to label it, how to store it, as well as how to maintain a suitable environment. Let us examine these topics.

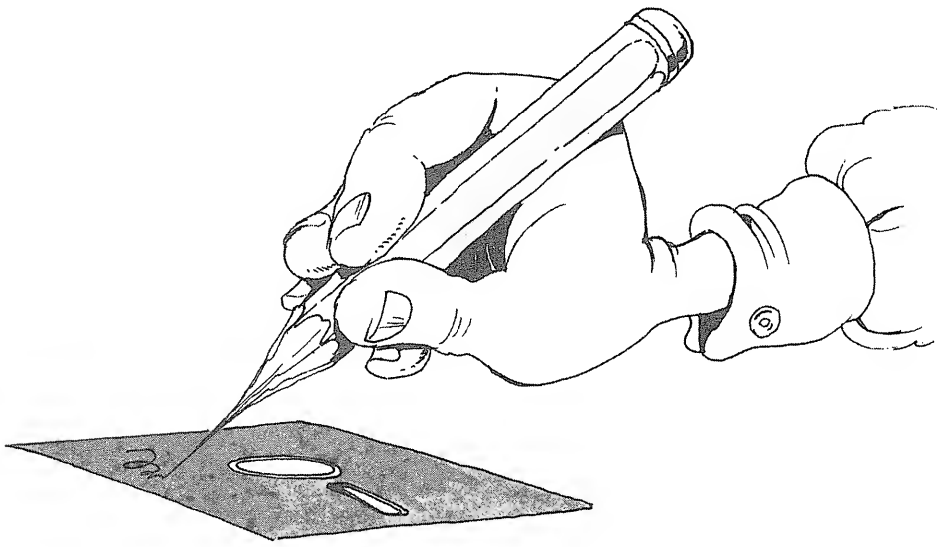
LABELING

Surprisingly, labeling can be a major source of problems for two reasons:

1. Hidden damage to the diskette can be incurred when writing on the label
2. Insufficient identification may result in misuse, erroneous filing or accidental erasure.

Let us examine these two problems in turn.

Writing On The Label



Remember: when writing on a label on a diskette, never use a hard pencil or ball-point pen. Pressure exerted on the label can damage the diskette underneath by either deforming the diskette or by pressing dust particles captured by the lining inside the jacket into the magnetic surface of the diskette. When writing on the label, use only a soft felt-tip pen. As a general rule, it is best to write on a separate label and *then* carefully affix that label to the diskette.

Also, don't use an eraser to erase a label. Residue from an eraser will find its way first into the envelope and from there to the magnetic surface of the diskette where it will cause damage.

Identify the Diskette

Whenever you modify the contents of a diskette, identify it properly. In time many copies of a file are created. Unless they are properly identified, much aggravation can result from using or destroying the *wrong* version. Immediately after use, always label each diskette with at least the following information.

1. the name of the file
2. the date

In addition, it is desirable to keep with the diskette a printout of its directory, i.e., the complete list of the files it contains. Generate this printout on the printer, then tape it to the envelope in which the diskette is kept.

Whenever possible, name files in such a way that successive versions can be identified. Start with LIST1, then call the second version LIST2, the third LIST3, etc. As long as you know what the latest version is, this works.

Beware of situations where several files are updated on the same diskette. You may no longer know which file was changed when. In such a case, create a separate backup copy of each file that was changed, or else carefully list each file along with the date it was last modified.

When a diskette is a master or a copy, identify it as such. Masters are normally kept in a separate location and handled with great care. Backup copies are also generally stored in a separate location.

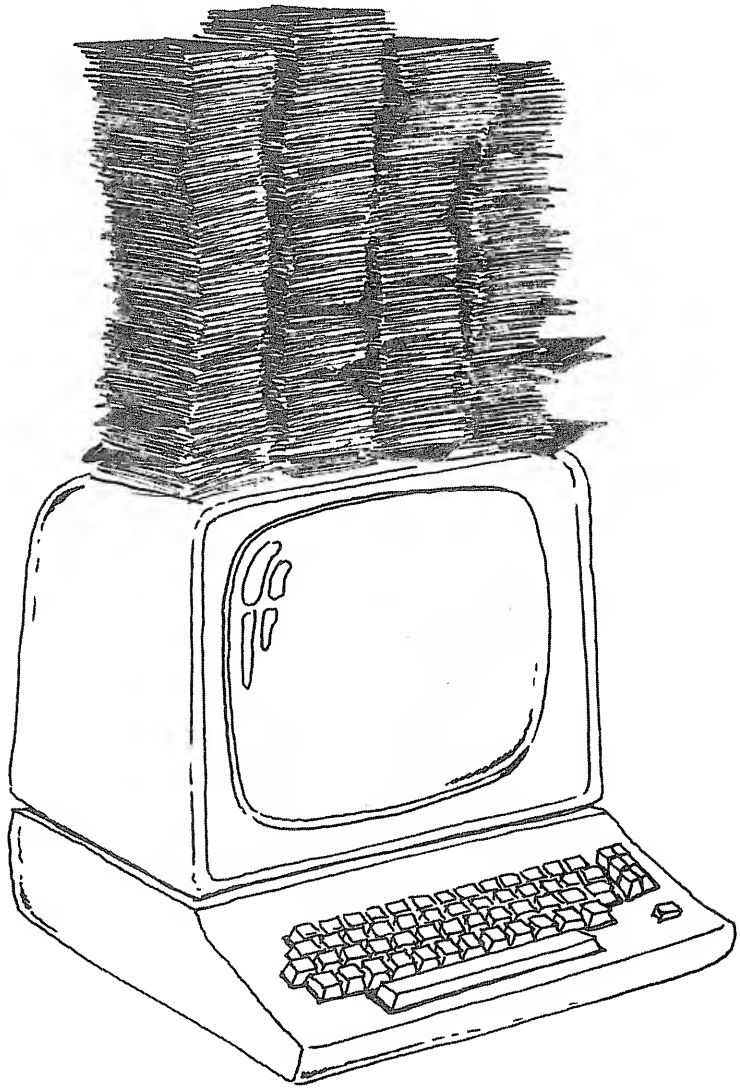
Dispose of obsolete copies after a reasonable period of time, or else:

1. You will quickly accumulate dozens of useless diskettes.
2. You may encourage errors by keeping old versions around.

STORING DISKETTES

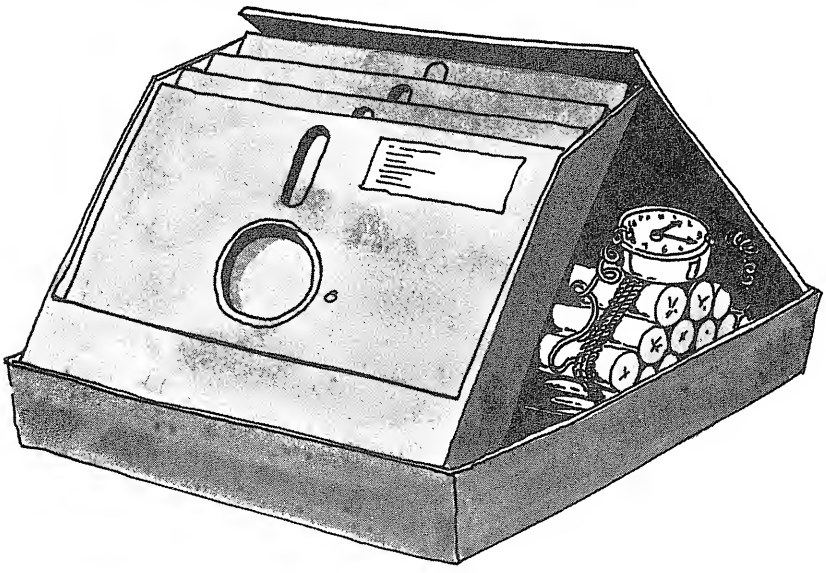
Both physical and environmental factors should be considered when storing diskettes. Diskettes can either be stored horizontally or vertically,

but they should not be stored in such a way that they will sag, slump, or be compressed. They should be protected from adverse magnetic or environmental conditions. Let us now examine the do's and don'ts for storing diskettes.



DON'T Let Them Lie Around

When not in use, a diskette should be stored in a protective envelope and preferably filed away. Leaving a diskette lying flat and unprotected on the top of your computer is an open invitation to disaster. Dust will accumulate on the diskette. Usually, no immediate effect will occur as the dust particles will be captured by the inner lining of the diskette. However, once more dust has accumulated, or pressure is applied to the lining of the disk jacket, one or more specks of dust will scratch the disk surface and damage data. Later on, when the data is used, because it is damaged, it will cause erratic system behavior and there will be no easy explanation for this behavior. Again, this is the time bomb effect.



DO Store Them Properly

When stored, diskettes should not be bent or stressed in any way. They may be placed in a box as long as there are no physical obstructions inside the box that might exert pressure on them. Don't overcrowd diskettes in a single container.

When storing diskettes horizontally, don't stack more than 10 diskettes on top of each other. Diskettes should not be compressed.

Diskettes may also be stored in vertical plastic holders. The advantage of plastic holders compared to metal ones is the guarantee that plastic holders are not or will not become magnetized. Such holders range in style from rotating diskette holders to plastic boxes (Figure 3.6) and vertical rack holders (Figure 3.7).

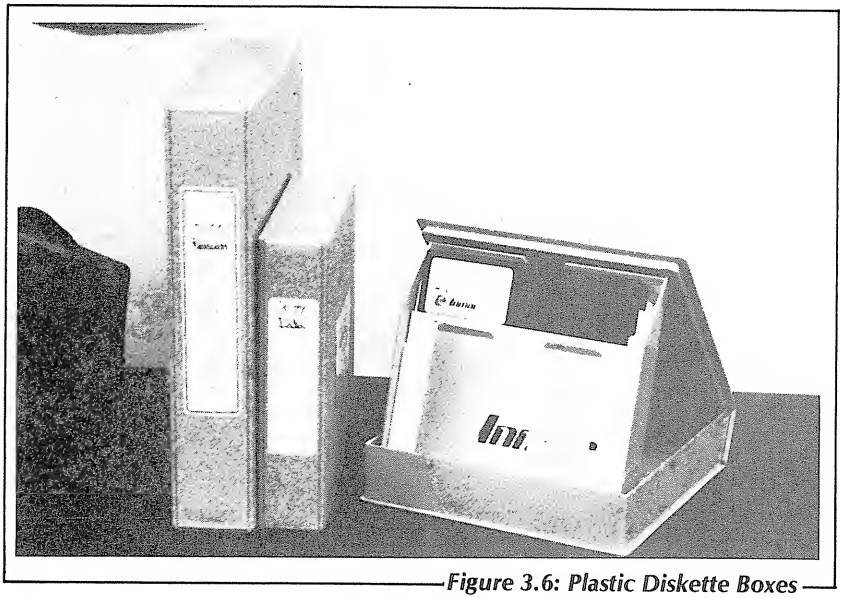


Figure 3.6: Plastic Diskette Boxes

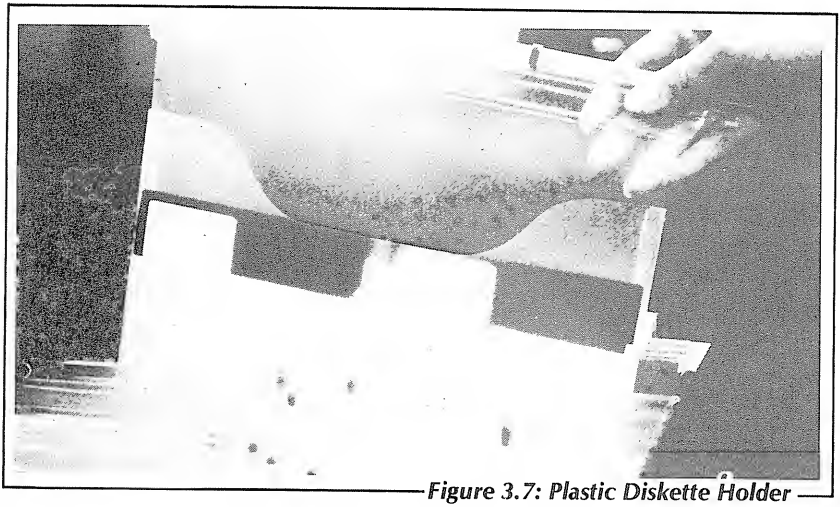
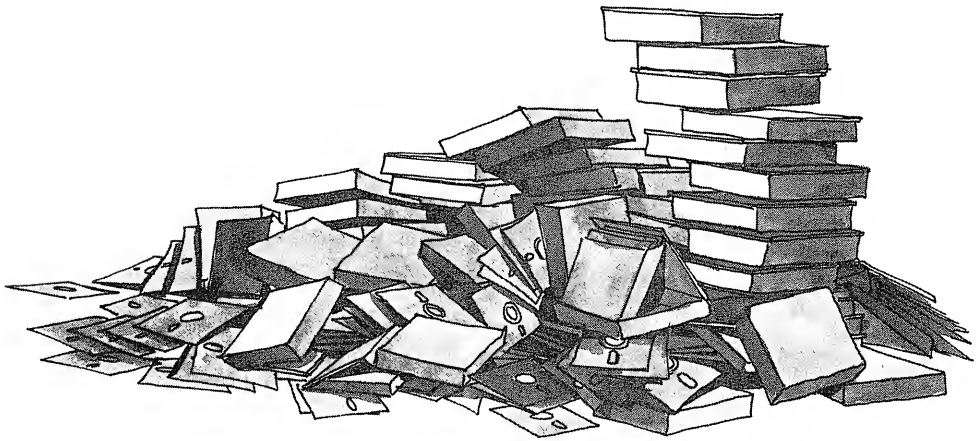


Figure 3.7: Plastic Diskette Holder

Using plastic will help prevent a magnetized metal element from coming in close proximity to the diskette, but it will not eliminate the danger altogether. In other words, a diskette lying in a plastic file holder may be wiped out if a magnetic coil or a magnetized screwdriver is placed near it. Therefore, the file holders themselves should be located away from sources of electromagnetic interference.

Hanging file holders may be placed in metal cabinets. Metal cabinets will, to some extent, shield the contents of a diskette from electromagnetic radiation. Naturally, this is true only if the metal cabinet is not magnetized.

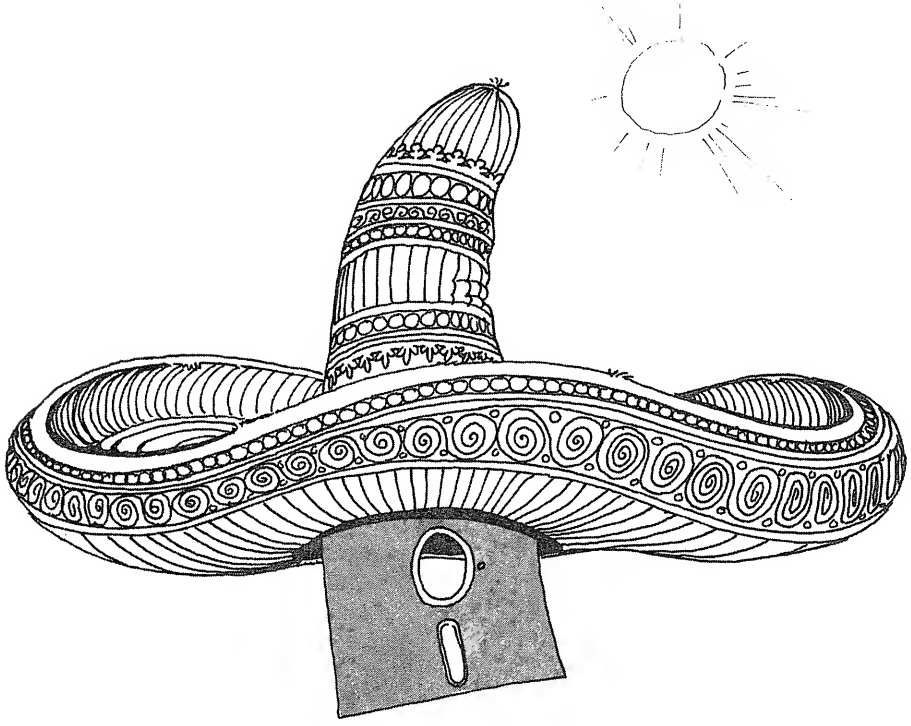


ENVIRONMENT

Diskettes must be used in a proper environment. Here are the main enemies of your diskette:

- temperature extremes
- dust
- liquids and vapors
- electromagnetic interference.

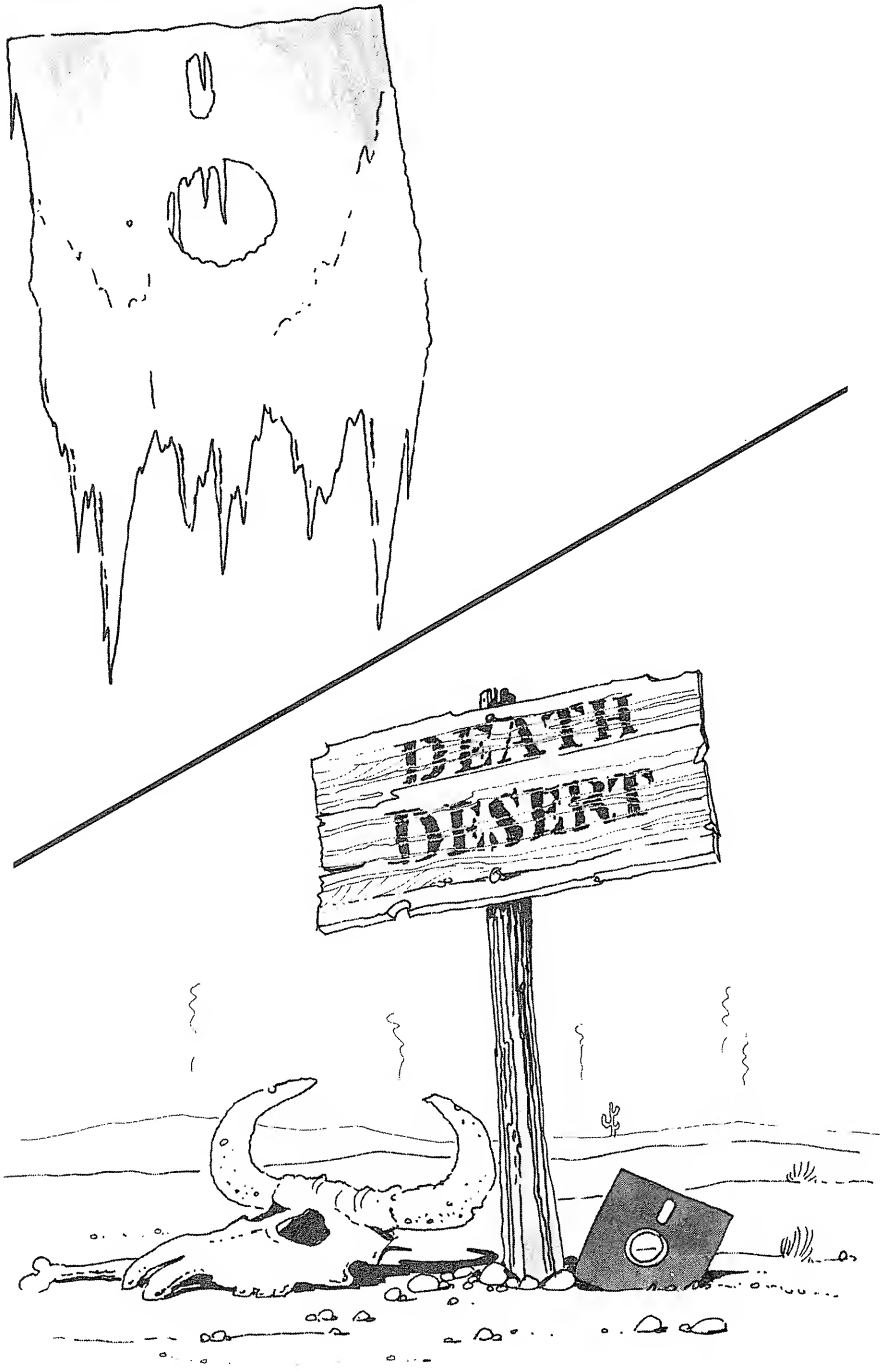
Let us examine each of these constraints in turn.



Temperature

Diskettes should be kept away from direct sunlight and extreme temperatures. Typically, diskettes will operate only between 10° and 50° Celsius (50° to 122° Fahrenheit). They will accept a relative humidity of 10% to 80%. If a diskette has been exposed to a temperature below 5°C or over 50°C (41°F or 122°F), it should be presumed damaged, and discarded.

Special high-performance diskettes can withstand higher operating and storage temperatures. They may operate from 10°C to 70°C (50° to 158°F) and may be stored at temperatures ranging from −40°C to 70°C


DEATH
DESERT

(−40°F to 158°F). Figure 3.8 shows unwarped high-performance diskettes placed in an oven next to damaged standard ones.

Don't use a diskette that has just been brought in from outside the building if there is a significant difference between the indoor and the outdoor temperatures. Allow a period of 24 hours for the temperature of the diskette to equalize with the temperature of the computer room.

Dust

Dust is one of the greatest enemies of diskettes. Dust may be due to an unclean environment or to more subtle causes such as heavy smoking, machinery (for example, drills used in dentistry), or specks of paper from a high speed printer. All sources of dust should be removed from the vicinity of disk drives.

Smoke in the air will also deposit particles on the surface of a diskette. This will cause the head to scratch the disk surface, thereby damaging the diskette.

Liquids

Liquids will damage the surface of a diskette. Don't use or even keep a diskette that has come in contact with a liquid. Discard it; it is unusable

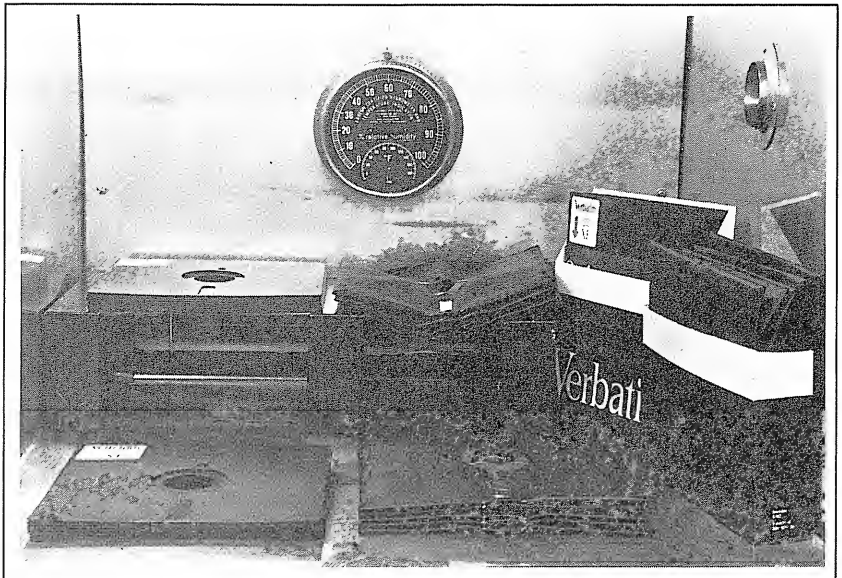
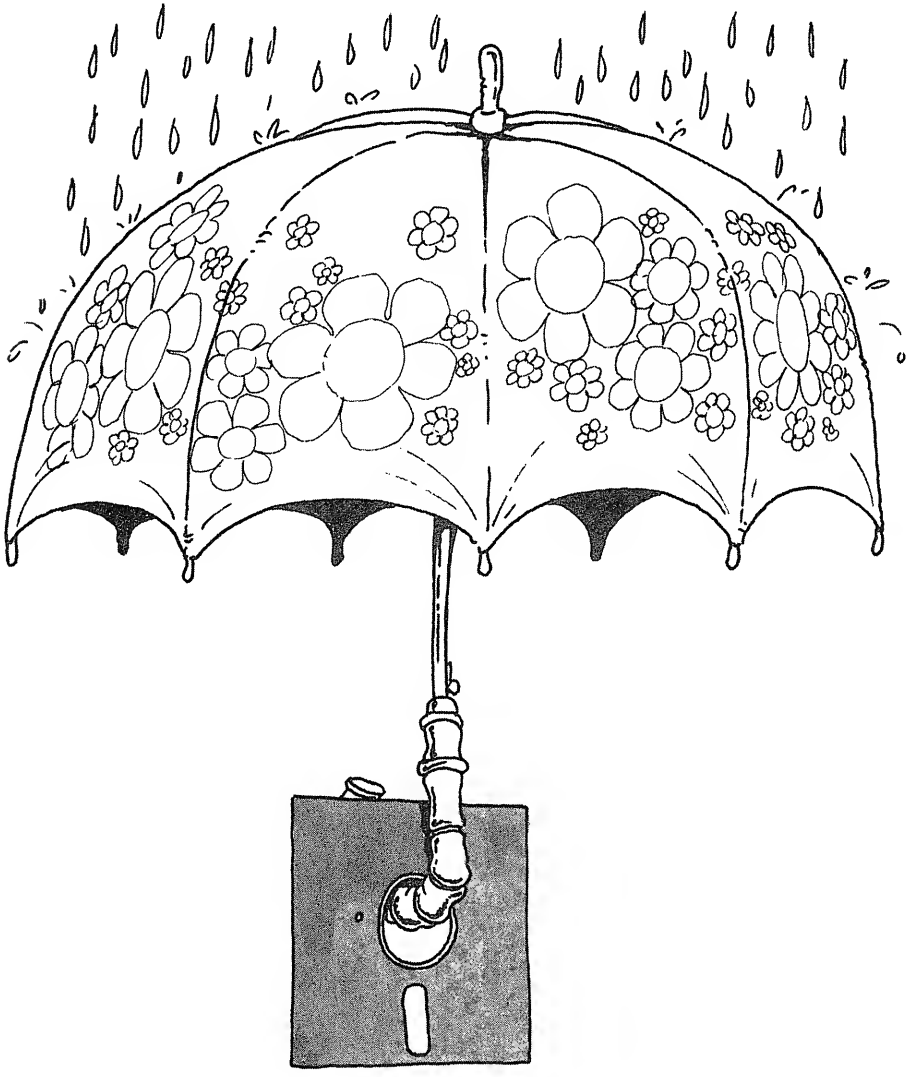


Figure 3.8: Extreme Heat Warps Standard Diskettes

even after the liquid has dried. The residue will contaminate the diskette. The best precaution is to ban all liquids from the computer room. Whenever this is not practical, care should be taken not to spill liquids on diskettes or on diskette jackets or envelopes.

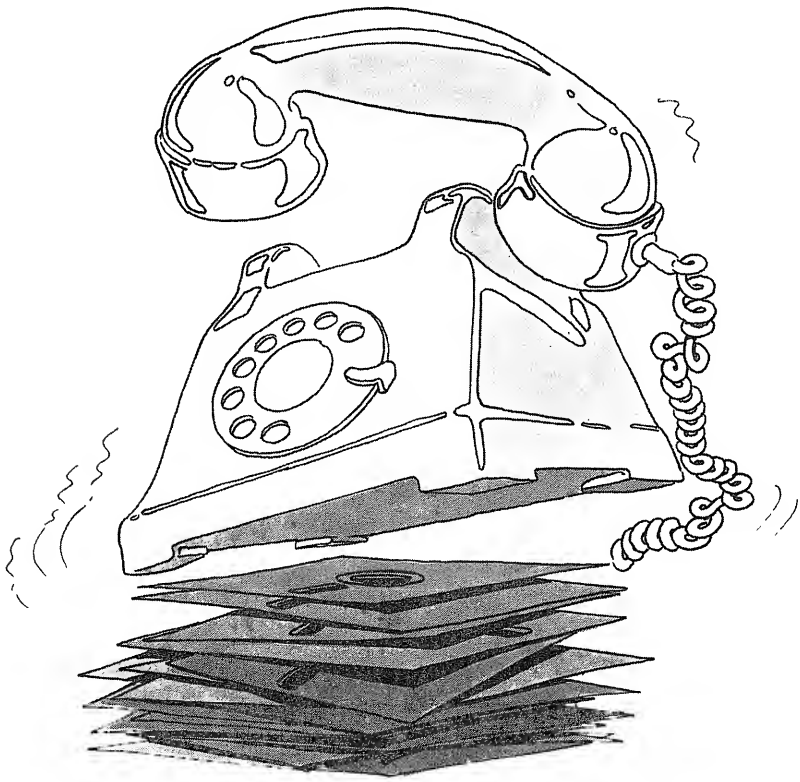


Vapors

Avoid placing solvents close to diskettes as chemical fumes may affect the magnetic coating of a diskette. Dangerous fumes encountered in office environments include fluids for duplicating machines, nail polish, and some adhesives.

Electrical and Electromagnetic Interference

Electromagnetic interference (EMI) is the name given to electromagnetic radiations that interfere with recorded data. Data can be destroyed or even wiped out entirely if a strong electromagnetic field or electrostatic field is applied to a diskette. Strong electromagnetic radiations are emitted by transformers and coils. A diskette should never be placed in close proximity to a magnetic coil (such as those used in telephones) or a degaussing coil (such as those around a color television tube).



Remember: don't put your telephone on top of a diskette, a box of diskettes, or even the disk drive. If the telephone rings while on top of a diskette or disk drive, it will wipe out any diskettes underneath it. (If you have any doubts, try it on an old diskette.) Keep the telephone cord short enough so that the telephone can never be inadvertently placed on top of disk drives or a work table where diskettes might be lying.

Any metal object should be suspected of being magnetized. In particular, screwdrivers and paper clips tend to become magnetized over a period of time. A magnetized screwdriver placed in close proximity to a diskette can damage the data. Similarly, car keys and other metallic objects may become sufficiently magnetized to affect a diskette. Always store diskettes in a proper container away from electromagnetic radiation.

Diskettes must also be protected from static. In a dry environment, static electricity can build up. In particular, if a computer room is equipped with wool carpeting, it is possible for up to 15,000 volts of static electricity to build up in the body simply by walking on the carpeting. If a finger is pointed at the computer or a diskette, an electrostatic discharge may occur and a spark will travel between the tip of the finger and the computer or diskette. A spark may also occur if you walk across the room and touch a metal part while holding a diskette. Such a spark is guaranteed to wipe out some of the contents of any diskette, as well as disrupt operation of the computer. To avoid this problem, you can use anti-static mats and sprays. Whenever the danger of static electricity exists (for example, on a dry day), either be careful not to point a finger at the diskettes, or be sure to ground yourself carefully before doing so. You can ground yourself by touching a metallic object connected to the frame of the building or by touching a neutral ground.

In summary, store diskettes in a cool, dry and clean environment. Don't abuse the physical or magnetic integrity of your diskette. Remove all sources of physical or electromagnetic danger from the computer room or at least keep your diskettes away from such dangers.

TRANSPORTING DISKETTES

Mailing Diskettes

Diskettes are often mailed. When mailing a diskette, use the best possible packaging that will guarantee the physical integrity of the diskette. Use rigid inserts in the envelope. If you use cardboard, make sure it is the corrugated kind. Place a sheet of it on both sides of the diskette, with the ridges of one

sheet perpendicular to the ridges of the other. Don't use ordinary cardboard, such as the back of a paper pad. It is not stiff enough and will bend, which may destroy data on the diskette. Whenever possible, place the diskettes inside the package, 1/4" to 1/2" away from the flat side. Distance is an excellent protection against pressure and magnetic objects.

Traveling with Floppies

Airport X-ray machines will not harm a floppy. However, the coils of the machinery surrounding them are dangerous. It is best to keep diskettes away from these machines.

PREVENTIVE MAINTENANCE

Two types of preventive maintenance action are recommended in order to safeguard your diskettes:

1. Keep your disk drive within the prescribed settings.
2. Use defensive procedures to maintain the integrity of your data.

Let us examine these two maintenance procedures in detail.

Maintaining The Drive

Disk drives must be correctly calibrated and aligned, i.e., the drive must be calibrated to the proper tolerance and the heads must be properly aligned. This is best accomplished by a specialist but can be done by a dedicated tinkerer. Special alignment disks are available from the manufacturer to facilitate this process. Typically, a drive will stay aligned for a year or more.

The disk drive heads should be cleaned regularly to eliminate dust. The frequency of cleaning depends on the environment in which the disks operate and the discipline of the users. As a rule of thumb, disk drive heads should be cleaned at least once a year. Special head-cleaning kits are available for this task. Preferably, solvents such as alcohol, freon or thinners should not be used.

Let's go through the steps involved in cleaning a read/write head using a kit. These steps are illustrated in Figures 3.9, 3.10 and 3.11. We will use a special head cleaning diskette coated with a special cleaning fabric.

Step 1: Saturate the cleaning fabric on the special diskette with the cleaning solution as shown in Figure 3.9.

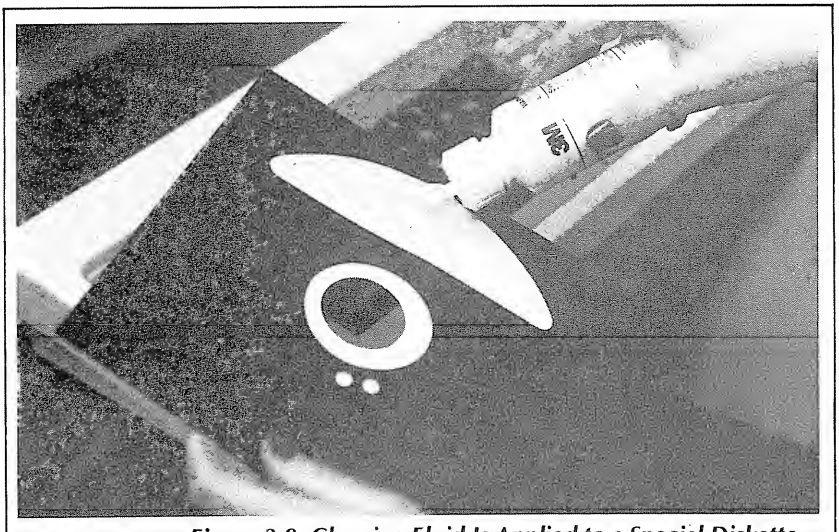


Figure 3.9: Cleaning Fluid Is Applied to a Special Diskette

Step 2: Insert the diskette into the drive (see Figure 3.10).

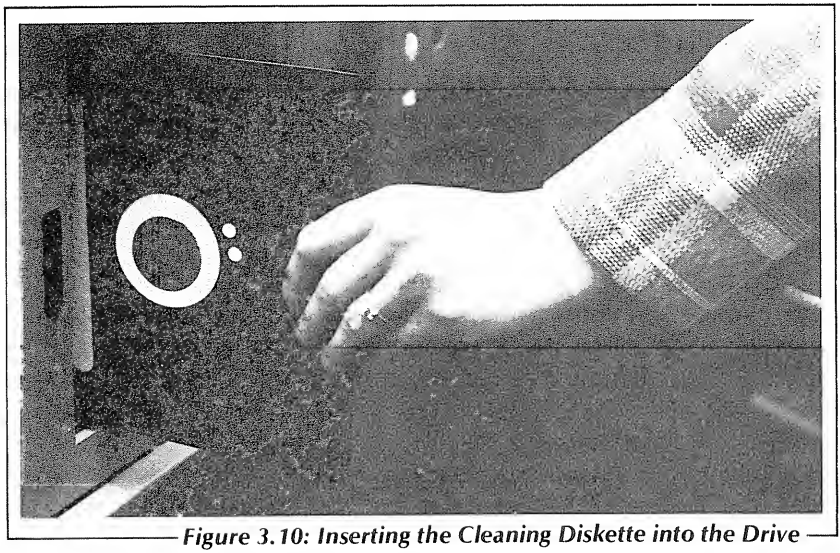


Figure 3.10: Inserting the Cleaning Diskette into the Drive

Step 3: After 30 to 50 seconds, remove the diskette and make a note on the diskette that it has been used. Typically, each diskette may be used up to 15 times (see Figure 3.11).

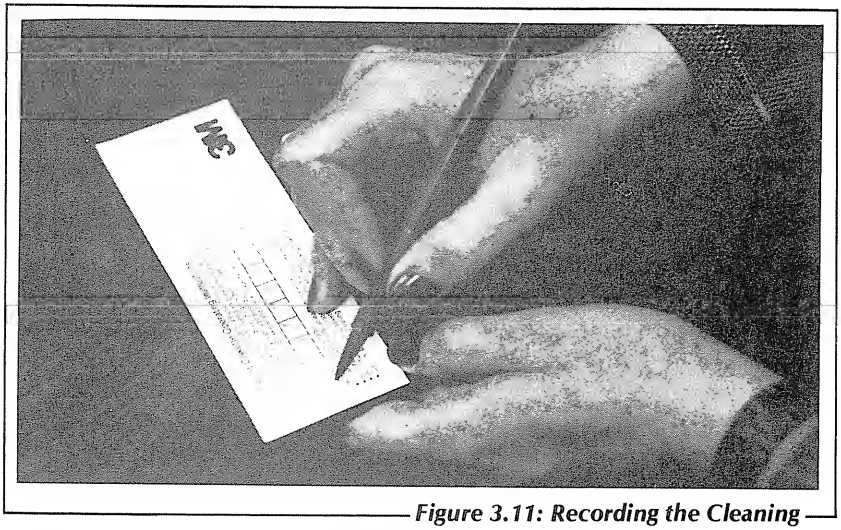


Figure 3.11: Recording the Cleaning

When double-sided diskettes are used, an extra opening may be found on the back of the cleaning diskette that can be helpful when cleaning the opposite side of the head mechanism (see Figure 3.12).

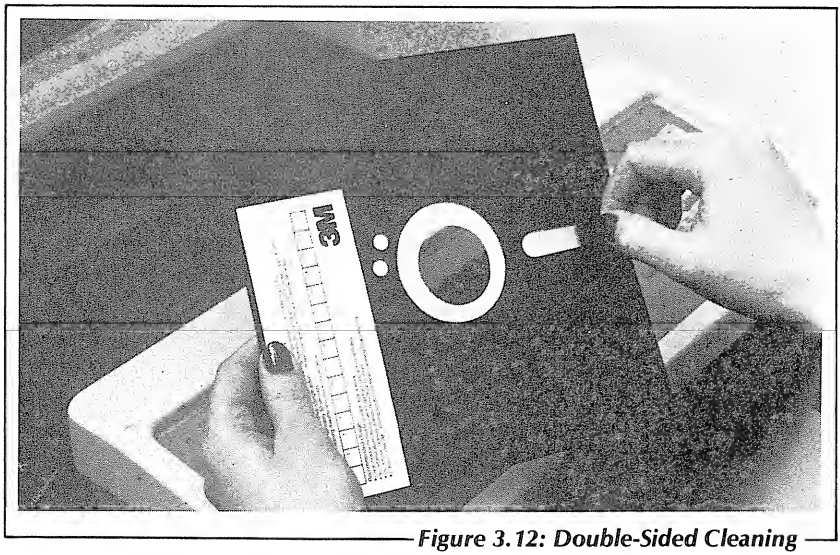


Figure 3.12: Double-Sided Cleaning

Half of the diskette contains a special cleaning fabric and the other half contains a regular dry fabric that wipes off the read/write head.

Depending on how frequently the diskettes are used, and the cleanliness of the environment, cleaning can take place every few weeks or months. Anti-contamination techniques, such as cleaning, normally have two main positive effects:

1. The read/write heads are kept contamination free.
2. Operators are reminded of the risk posed by dust and other particles to their equipment and will generally become more cautious.

A typical list of disk contaminants includes: dust, other particles, hair, skin flakes, fingerprint oil, and smoke film.

Dual-sided diskettes are much more susceptible to dust than single-sided diskettes. With a single-sided diskette, the ceramic read/write head presses on one side of the diskette while a soft felt backing presses on the other side. Compression of the diskette material is minimal. In the case of a dual-sided diskette, two ceramic read/write heads are applied to the diskette simultaneously, one on each side.

Don't attempt to clean the diskette surface itself. Any contact with the disk surface will contaminate it.

Remember also that disk drives are sensitive mechanical devices. When moving a disk drive, be careful to avoid shocks and vibrations. Such physical disturbances might misalign the head.

Physical damage to a diskette is inflicted either by the drive or the operator. Diskettes should be frequently inspected for signs of wear or damage. If there is visible wear or damage on the disk surface, the disk should be presumed bad and should no longer be used. A backup should be used instead and the suspected disk should be discarded. Remember, the appearance of large shiny rings may indicate a mechanical problem with the disk drive.

Most diskettes become damaged before they wear out. However, in circumstances where diskettes are valuable and are frequently used, center rings are available and can be used to reinforce the spindle holes of diskettes.

DISK FAILURES

Diskette failures will seldom occur if proper handling procedures have been followed. If a diskette has been handled properly, and a disk drive failure occurs, improper calibration or alignment should be suspected.

Let us examine disk errors and possible causes.

Disk Errors

Disk errors are due to the accidental change of the value of one or more bits of information at its surface. Such errors are traditionally classified in three main categories:

1. *Drop-Outs.* In this case, bits are wiped out either because of a defect on the disk surface or because of an inadequate write signal generated by the read/write head. Both cases are generally attributable to contamination or to physical damage to the diskette.

2. *Drop-Ins.* In this case, spurious bits are written in locations where they should not be. This is generally due to electromagnetic interference where a strong magnetic field creates spurious information on the surface of the disk. This can also be due to disk drive malfunction or to erroneous software that writes information in a place it is not supposed to.

3. *Bit Shifts.* This problem refers to the physical shifting of bits of information at the surface of the disk. Such shifting results in timing errors that

may make the data unreadable. This type of problem is generally caused by electromagnetic interference, but it may also be caused by physical distortion or high temperature.

Most disk errors are detected during the reading process. This happens because the data that was stored on the disk has been damaged ("polluted"). Usually, the data contained in the affected file on the disk has been lost. In any case, the contents of the entire disk should now be suspected, and the polluted diskette should be replaced by the backup.

However, if a failure occurs while writing, three causes should be suspected before accusing the equipment:

1. The write-protect tab may not be properly positioned over the notch (or removed from it, in the case of a minidiskette).
2. There may be a software protection feature in the operating system that prevents unauthorized writing on a given file.
3. You may be using the wrong type of diskette for the disk drive. In particular, a hard sectored disk will not work with a soft sectored disk drive.

FLOPPY DISK SUMMARY

Floppy disk failures are the most common cause of failures for small computers. Proper diskette handling requires respect for the physical and magnetic integrity of the diskette. As long as proper handling precautions and proper operating procedures, including a thorough backup procedure, are followed, diskettes will operate reliably for long periods of time.

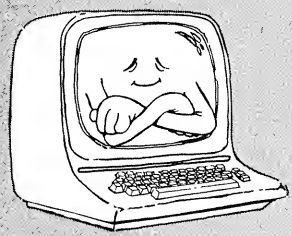
CHAPTER 4
HARD DISKS

Discipline is the mother of success.
— Aeschylus

FOR THE HOME COMPUTER USER

The main recommendation is:

Avoid dust.



INTRODUCTION

Hard disks are used in most business applications where several million bytes (i.e., characters) must be directly accessible. Although they cost more than floppy disk drives, hard disk units offer a much higher capacity, and a faster access time to the information they contain.

UNDERSTANDING YOUR DISK

We will first describe how a hard disk operates and the various types of disks that exist, including backup units. We will then examine how to use a disk and how to store it properly.

Disk Operation

As its name indicates, a hard disk is a disk made of a hard but light material that has been coated on both sides with a magnetic oxide. It is usually encased in a special protective shell or in a cartridge. Each disk has a large hole in the center so that it can be inserted on a spindle.

A typical disk platter rotates at a high speed (such as 2400 rotations per minute (rpm) or 40 rotations per second). Unlike a floppy disk, the read/write head does not make contact with the disk surface; it flies over it. The read/write head has a special aerodynamic profile and floats on an air cushion just over the disk surface. The equivalent linear speed of the disk platter is around 60 miles per hour (100 kilometers per hour). At such a high speed, an air cushion effect can be achieved and the head is said to float. If the head should ever come in direct contact with the disk surface, the disk surface would be irreparably damaged. This is one of the worst accidents that can occur in a disk drive. It is called a "head crash." Most of the advice given in this chapter is aimed at preventing "head crashes."

Disk Sizes

Hard disks come in various sizes, usually ranging from 5-1/4 inches to 12 inches in diameter. They can, however, be larger. The larger the disk, the larger the amount of data it can hold. However, the larger the disk, the more costly the disk drive.

A typical hard disk holds 10 megabytes of information on its two surfaces. Information is magnetically recorded in a binary format, i.e., as a sequence of 0s and 1s, on concentric tracks of the disk. The number of tracks

on each disk depends on the size of the disk and the manufacturer. As an example, a disk may have 408 tracks (the outermost track is called track 0), and 48 sectors per track. Typically a sector contains 256 bytes.

Let's compute the number of bytes per surface for such a disk: 408 tracks × 48 sectors per track × 256 bytes per sector = 5,013,504 bytes per surface or 10,027,008 bytes per disk for both sides. This is a 10 megabyte disk.

We will now examine each type in turn. For comparison, Figure 4.1 shows from left to right drives for the SA4000 14-inch hard disk, the SA1000 8-inch hard disk, an 8-inch floppy, and a 5-1/4-inch minifloppy.

Types Of Hard Disks

A typical disk unit is shown in Figure 4.2. Disks are commonly assembled in stacks of *platters* in order to increase their storage capability (see Figure 4.3) and are called *disk packs.* Disks may also be packaged in removable cartridges. A *disk cartridge* is shown in Figure 4.4. Finally, sealed units are used for the recent *Winchester disks.* A Winchester disk drive is shown in Figure 4.5.

Disk Packs

Disk packs come in 5- and 12-platter packs. A 5-platter disk pack typically contains 25 to 80 megabytes. A 12-platter disk pack typically contains 100 to 300 megabytes. Because there are several platters inside each

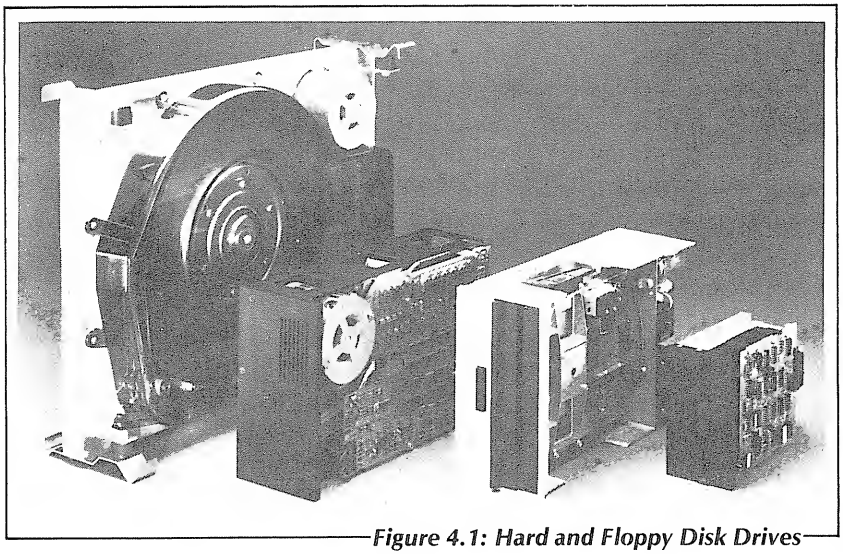


Figure 4.1: Hard and Floppy Disk Drives

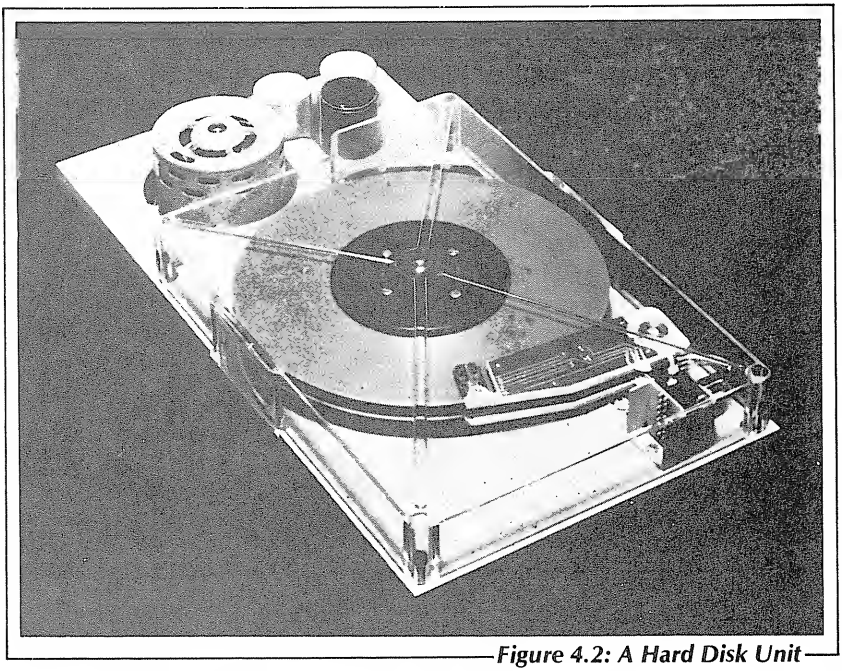


Figure 4.2: A Hard Disk Unit

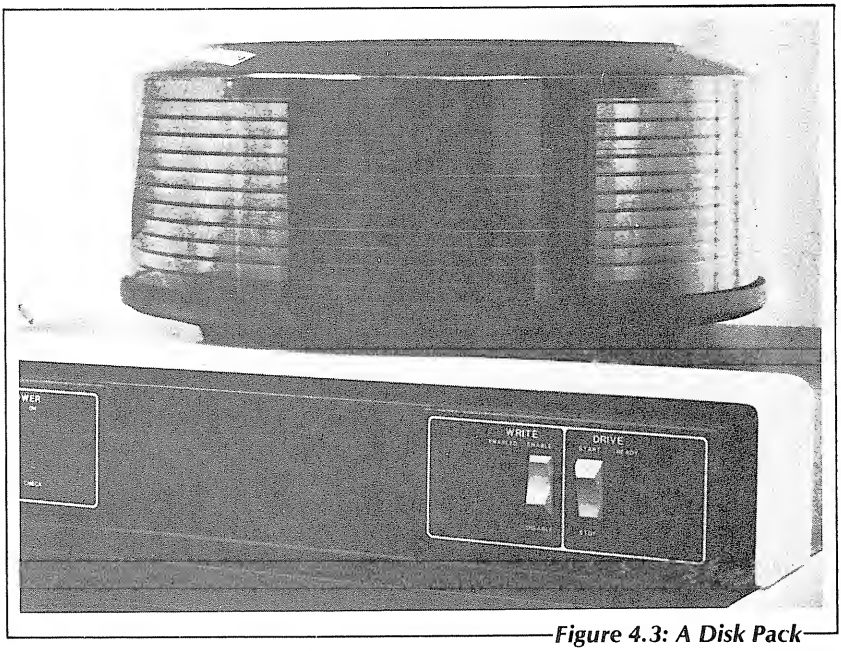


Figure 4.3: A Disk Pack

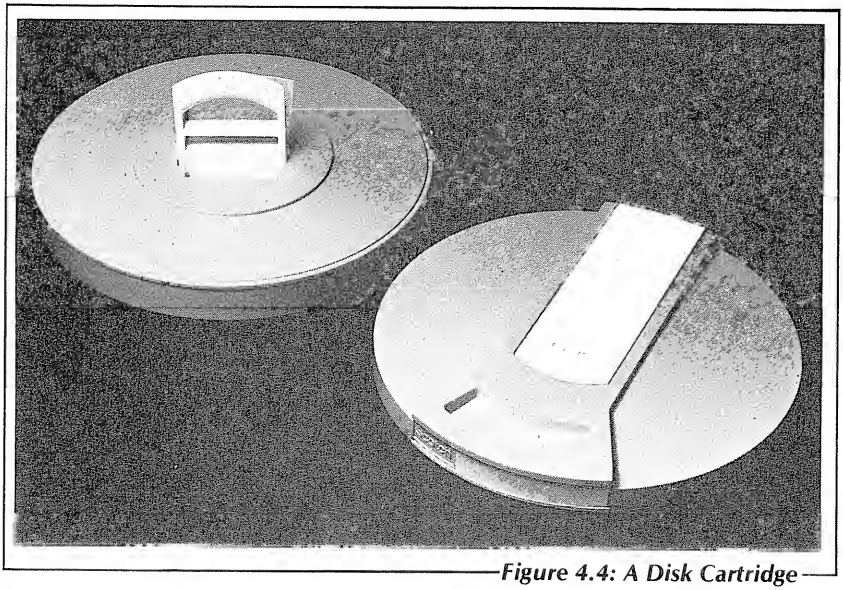


Figure 4.4: A Disk Cartridge

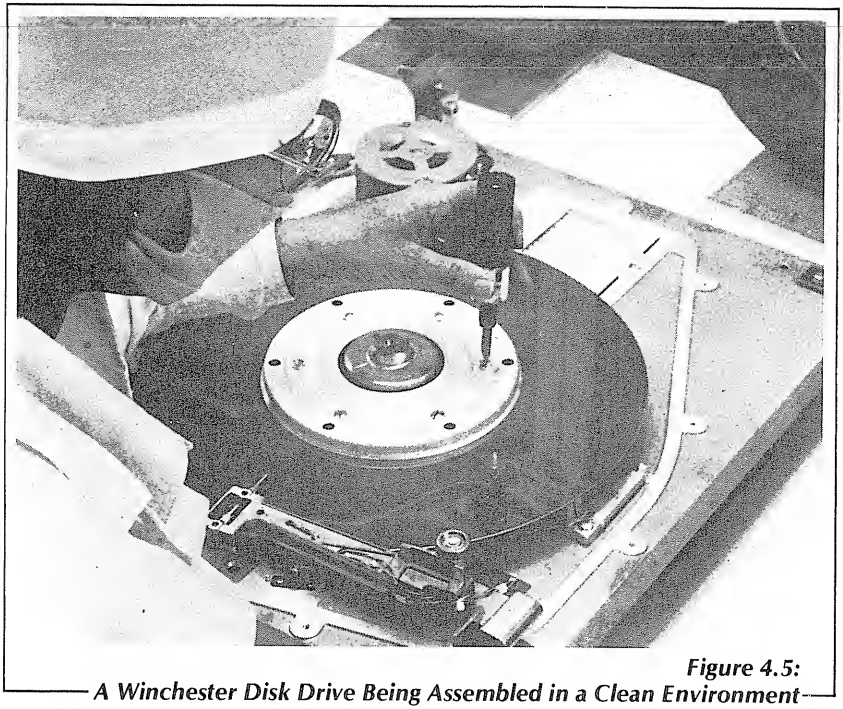
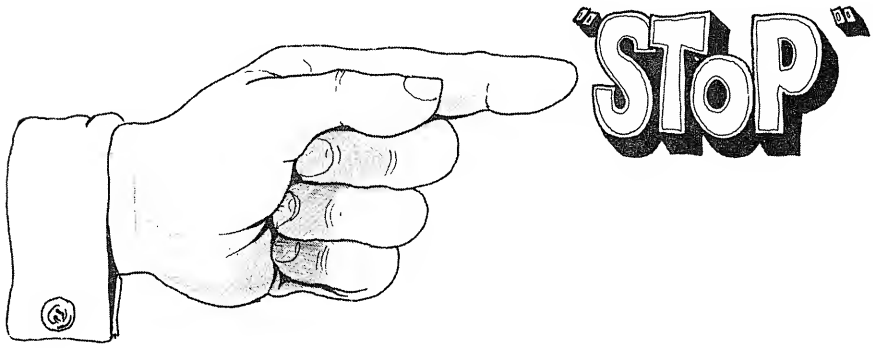


Figure 4.5: A Winchester Disk Drive Being Assembled in a Clean Environment

disk pack, they should be inserted and seated more carefully than disk cartridges. The following recommendations apply:



- Once the pack has been installed on the drive, gently turn the cover as far as it will go to guarantee that the disk pack has been properly seated. (Be gentle.)
- When loading the disk pack, don't let the disk drive spindle strike the platters, or misalignment will result.
- When removing and replacing the top and bottom covers of a disk pack, don't allow the covers to touch the platters.
- And of course, don't touch the platters with your fingers.

Removable Cartridge Disks

A disk cartridge offers the advantage of small size and portability. It is generally combined with a fixed disk in a single disk drive.

Cartridges that look similar may actually have a different number of sectors. Generally it is possible to count the number of sectors in the following ways:

- In the case of a *front-loading cartridge,* the sector notches can be counted by examining the area rotating close to the hub. The number of sectors is equal to the number of notches minus one.
- In the case of a *top-loading cartridge,* the bottom cover must be removed. Then the number of notches can be counted by examining the metal hub. Again, the number of sectors is equal to the number of notches minus one. Promptly replace the bottom cover.

Traditionally, in the world of minicomputers and larger computers, hard disks come in dual disk units:

- The first disk is a fixed platter that is non-removable.
- The second disk is a removable cartridge.

Typically, the operating system and all installation programs are permanently stored on the fixed platter, while data files are stored on the cartridge.

At the end of each day, the contents of a disk may be backed-up on a fresh cartridge. Whenever an entire cartridge needs to be backed up, the process may become somewhat complicated if the fixed disk is full or if it holds several programs.

To transfer files from one cartridge to another, ideally, two cartridge drives should be available, or else the file must first be copied to the fixed platter, then transferred to a fresh cartridge. Thus, it may be necessary to load and unload each cartridge several times. When it is necessary to copy entire disks frequently, two disk cartridge units should be installed.

Disk cartridges are relatively inexpensive and easy to carry. Two cartridges can be easily fitted into a special carrier about the size of a large attache case. Cartridges are widely used on small computers.

Winchester Disks

Winchester disks were introduced in 1978 as low-cost, low-speed hard disks. Winchester disks rotate inside a sealed enclosure, which substantially reduces the danger of contamination (see Figure 4.6). Winchester disks are lower in cost than regular hard disks; however, their performance level is also lower. The smaller Winchester disk drives (8-inch and 5-1/4-inch) take up the same amount of space as their floppy disk counterparts, but they operate faster and a Winchester disk has a greater storage capacity than a floppy. Winchester disks are therefore commonly used on low-cost microcomputers.

Because Winchester disks usually come as single-disk units, they must be backed-up by a separate, removable mass-storage device. Standard magnetic tape and streaming tape units are commonly used for this purpose.

The Backup Problem

The main advantage of a hard disk is its large storage capability. The main disadvantage of a hard disk drive is that a large amount of data may

be lost in the event of malfunction. Because of the large storage capacity of a hard disk, it is imperative that files stored on a hard disk be saved at frequent intervals. This is known as backing-up the disk.

The contents of a hard disk should be backed-up at least once a day, and more frequently if necessary. Because of the large storage capacity of a hard disk, only two devices can be used to back it up: another hard disk (a cartridge unit) or a magnetic tape. Using another medium, such as a floppy disk, for making a backup is theoretically possible, but highly impractical. Let us examine the three alternatives for backing-up a disk.

Of the three alternatives, a removable disk (cartridge or disk pack) is the fastest to use, but relatively expensive. A removable cartridge is generally used on small business systems for two reasons:

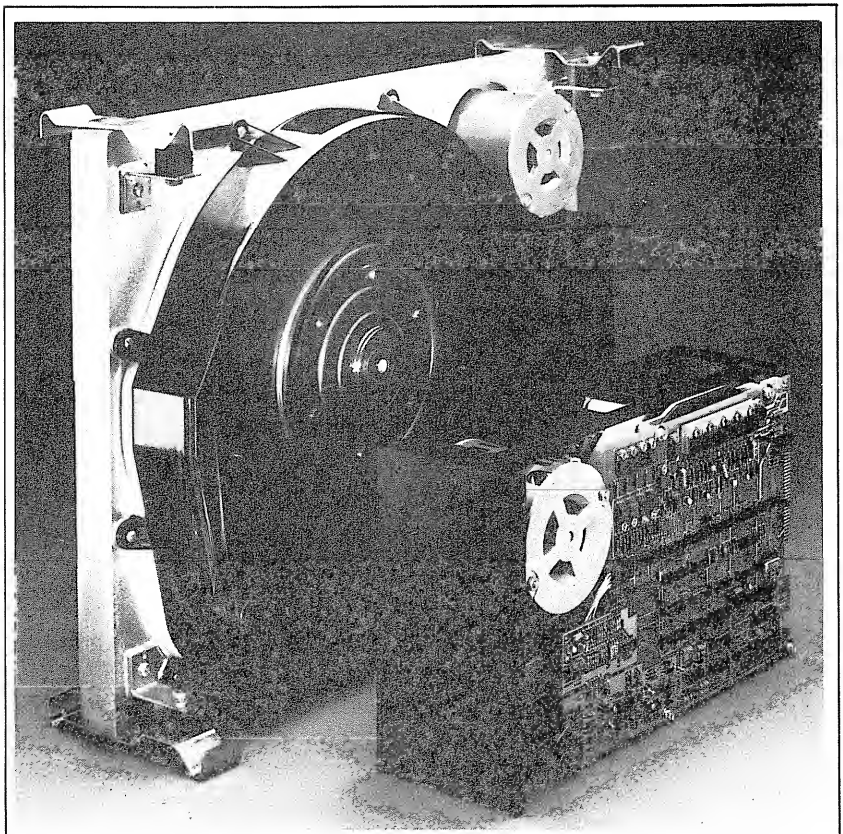


Figure 4.6: Winchester 14-inch and 8-inch Disk Drives

1. The cartridge disk drive is already part of the disk unit; therefore no additional device is required.
2. The amount of information to be saved is generally small; therefore a single cartridge per day is usually sufficient.

A disk pack is also fast, but it is more expensive. It is used only if a large storage capacity is required, and if speed is a consideration.

Magnetic tape is slower to use, but inexpensive and has a large capacity. This is the device used by most medium to large installations. The initial cost is higher, since a tape unit cannot be used as a substitute to an on-line disk unit and must be added to the system, but the recurring cost is lower.

Floppy disks are generally impractical in view of the volume of information to be saved. They do, however, cost the least, and are sometimes used by the smallest installations.

Proper backup procedures will be described after we have learned how to operate and store a hard disk.

USING HARD DISKS

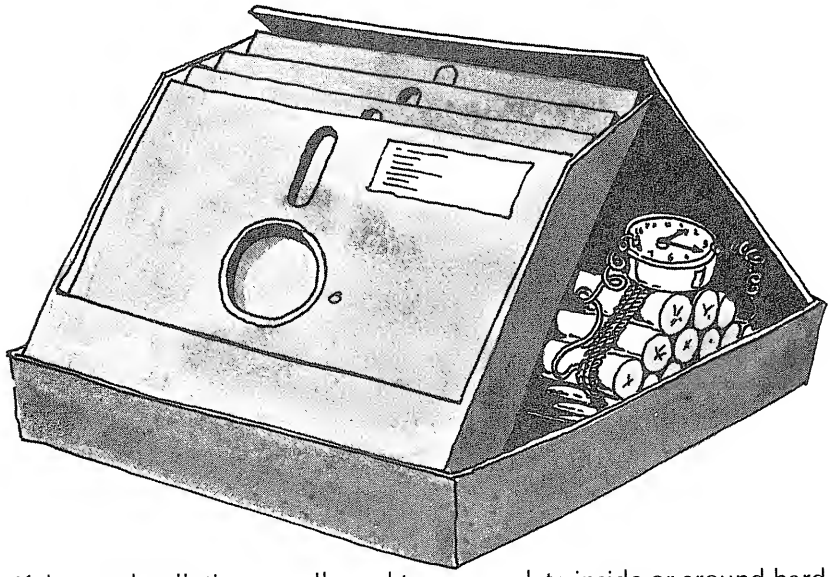
We will now examine the environmental requirements for safe disk operation. First, dust and pollution, the greatest enemies of a hard disk will be discussed, then temperature and electrical power.

Environmental Requirements

As in the case of floppy disks, the most important rule when using hard disks is to respect the physical and magnetic integrity of the disk. However, because of the high rotational speed and high density of information on the surface of the disk, the requirements are more stringent for hard disks than for floppy disks.

Dust and Pollution

Figure 4.7 illustrates the low tolerance level that a hard disk has for external pollution. Any particle on the surface of a disk will cause damage to the surface and/or the read/write head. Data will be destroyed and it will be impossible to recover the data using traditional methods. In addition, if the read/write head has been scratched, the entire disk unit becomes unusable. Protection against dust and pollution is therefore the prime consideration when using a hard disk. The use of a closed circuit air-conditioning unit with an efficient filtering system is almost a mandatory requirement when using hard disks.



If dust and pollution are allowed to accumulate inside or around hard disks, the "time bomb" effect (described in Chapter 1) will be created. A single particle of dust or smoke can remain lodged on a disk for days, or even months. If the disk or, more specifically, the area of the disk on which the dust particle rests is not used, no visible ill-effect will immediately occur. Eventually, however, the particle will come under the read/write head and cause a crash. Then it will be too late, and the data will be lost. The damage can be even more subtle. For example, the dust may not settle directly on the surface of the disk. Instead, it may penetrate inside the disk mechanism and become lodged somewhere in that mechanism. Later—perhaps months later—the dust may fall onto the surface of the disk and damage it.

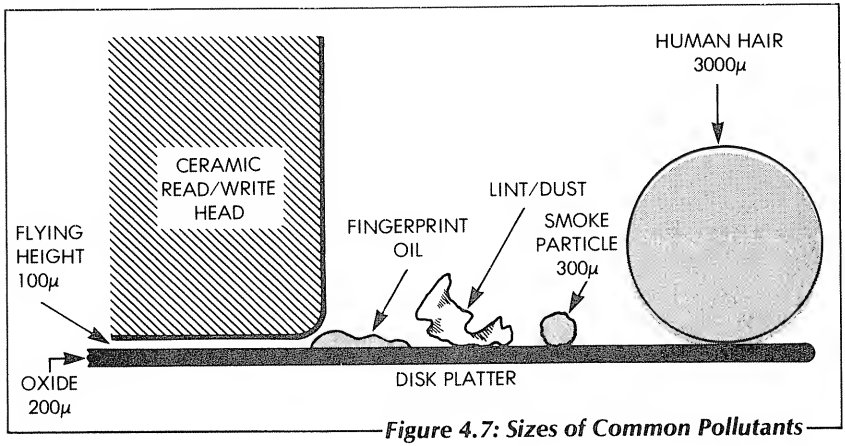
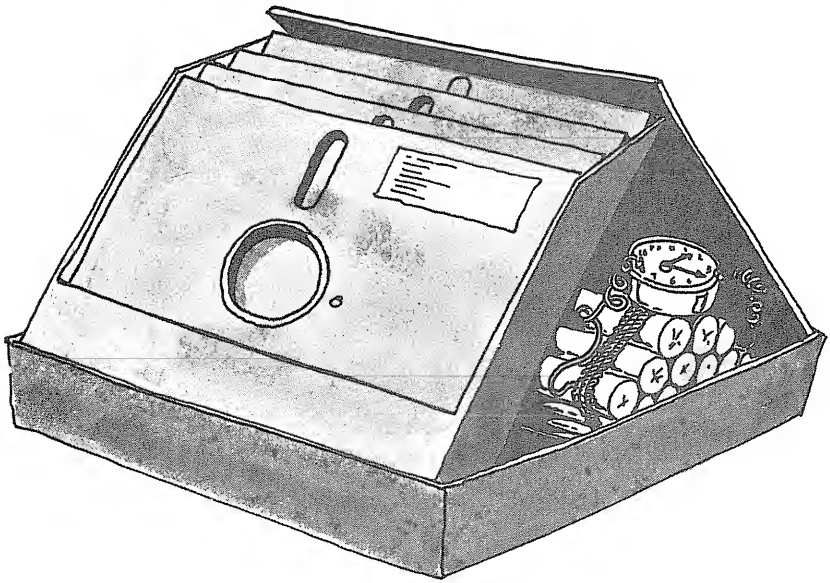


Figure 4.7: Sizes of Common Pollutants

Once you have gone through an unexpected disk crash, you will probably be a firm believer in the fact that the cost of maintaining a dust-free environment in the computer room is well worth it. Remember that a head crash is about the worst danger to your system short of a fire. In some cases, aluminum particles will be sent flying throughout the drive, causing short-circuits and possibly a fire.

A dust-free environment is normally achieved by using a recirculating air-conditioning unit with a high-efficiency dust filter (one that achieves at least 90% efficiency with standard dust). However, in highly polluted areas, the filtering capability of the unit should be even higher. Frequently check the dust filters on your disk pack and air conditioner (or other similar unit) for dust accumulation.

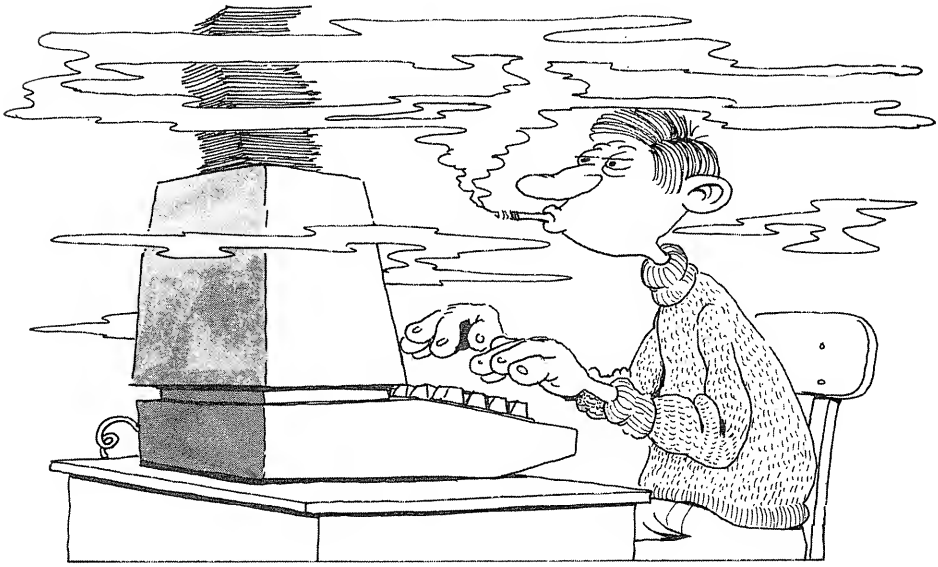


If you are not using an air-conditioning unit and have not experienced any head crashes, don't assume that your specific disk unit is immune to dust. In all likelihood, you will probably experience several head crashes in the future. You might not experience them until after the system has been operating for a year. After that time, however, they will probably occur relatively frequently as dust will have accumulated in various locations throughout the room, the computer system, and the disk drive itself.

Remember: The recommendations concerning dust particles also apply to smoke particles. Good air filters will generally remove most smoke particles from the air. However, as the filter deteriorates, smoke will penetrate

inside the disk mechanism. Therefore, it is best to forbid all smoking in close proximity to a hard disk.

The other main environmental considerations are temperature and power. Let us examine them in turn.



Temperature Equalization

Hard disks must be equalized in temperature prior to use. After you insert a removable cartridge in a unit equipped with a fixed platter and a separate removable cartridge, the disk drive will normally not operate until both disks arrive at the same temperature. Such units usually have an Auto/Wait feature.

Because of the high data density on the surface of the disks, the physical distortion caused by different temperatures is sufficient to prevent the correct reading and writing of information. If you anticipate using a disk frequently, it is best to store the disk in the computer room.

The following rule applies to both floppies and hard disks: don't use a disk that is brought into the computer room from the outside (or from a location that is substantially different in temperature) for at least 24 hours. This will allow time for a correct equalization of temperature.

As an emergency procedure, if it should become necessary to rapidly use a disk that comes from outside the building, the disk can be placed

inside the drive and rotated for 5 to 30 minutes, or more. Spinning the disk inside the drive will quickly bring it to the same temperature as the other parts in the drive. However, this procedure is generally not recommended as it can lead to additional problems such as modifying the temperature of the fixed disk and causing condensation because of the rapid change in temperature.

Disks are quite tolerant in terms of humidity and electrical power, but not in terms of temperature. Keep in mind that:

- 10% to 80% relative humidity is acceptable.
- The usual power range is 115 volts (or 220 volts) plus or minus 10%.
- The usual operating range is 55°F to 100°F (12°C to 38°C).
- Typical heat dissipation by a dual disk unit is 1500 to 2500 btu per hour.

Power Out

A power failure is one of the worst potential dangers to your disk unit. In principle, once the power goes out, control of the disk unit is lost, and there is a possibility that the head might crash as the disk slows down. In practice, all well-designed computer systems account for this potential catastrophe. In a well-designed system, as soon as a drop in line voltage is detected within the computer, or within the drive, a special program or mechanism, called an "orderly shut-down routine," will take over. It will lift the head away from the surface of the disk, and lock it in place. Normally, if there is a power failure, the disk door or lid will remain locked. Once power is reapplied, the disk will resume normal operation. The program that was in execution at the time of the power failure will be lost and any files on which it was operating will be in an indeterminate state.

Some of the newer low-cost systems are not equipped with an orderly shut-down routine. Unfortunately, if a power failure should take place, head crashes may occur. The absence of a shut-down routine may be sufficient cause for not purchasing such a system unless the disk drive itself is equipped with a mechanism that will automatically retract the head in the event of a power failure.

Liquids

Any contact with a liquid will damage a disk permanently. This includes condensation, which should never be allowed to occur. If liquid is allowed

to remain on the surface of a disk, the disk itself will be permanently damaged and the read/write head will be contaminated.

Backing-up

The recommended procedure is to back-up a hard disk at least once a day if it is in use. A sophisticated operating system will automatically make a backup copy of a file whenever the contents of the file are altered. Many others will not, and this task must then be performed by the user.

When a backup has been made on a disk pack, disk cartridge or tape, remove it and store it away. Backups are generally stored in the computer room. This guards against possible disk damage or malfunction, but it is not sufficient from a security standpoint. Extensive damage due to fire, heavy pollution, or deliberate human sabotage may occur within the computer room itself, damaging not only the disk in the disk drive but also the backup disk or tape. It is, therefore, highly recommended to make a secondary backup of all files in the computer room on a portable storage medium (either disk cartridge or tape) once a week (or, at least, once a month) and to store this secondary backup medium in a safe, remote location. A safe location might be a fire-proof vault, located (preferably) away from the building itself, in a location not accessible to computer room personnel.

Storing Hard Disks

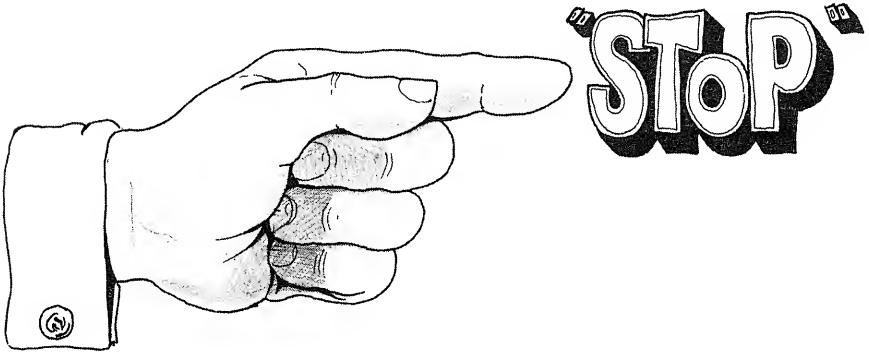
Disks should not be touched, dropped, or subjected to vibrations. They should be stored in properly designed disk racks. (See Chapter 9 for details.) Disks should be kept in a dry, safe, pollution-free place. They

should be stored in a secure place where they will not be subjected to vibrations. Ideally, disks should be kept in the same room or in close proximity to the computer room to avoid variations in temperature.

One additional, important recommendation is to keep the disks in an easily accessible storage rack or cabinet, in order to reduce the probability of dropping one. This will prevent damage to the disks due to physical shocks. Disks should be stored at temperatures that remain within the manufacturer's permissible range. Typically, this range is 50° to 125°F (10° to 52°C).

Never keep your disk packs in a car trunk. If they must be carried outside, carry them in a specially designed container to avoid shocks, vibrations, and extremes in temperature. Exposure to freezing temperatures will also permanently damage the disk. Exposure to high temperatures will damage either the data on the disk or the disk itself.

Information is stored in magnetic form on the surface of a disk. As in the case of diskettes, any strong magnetic field will alter or destroy this information. The following recommendations apply:



- Don't place disks near strong magnetic fields. Removable cartridges should be stored in proper disk racks.
- Don't place a telephone directly on top of a disk pack as this may damage data inside the pack when the phone rings.
- Take precautions to avoid static electricity discharges.

Cleaning Disks

Disk surfaces should be cleaned periodically. This preventive maintenance removes dust, dirt, loose oxide and other foreign particles that might cause improper disk operation.

A special pad or wand saturated with isopropyl alcohol may be used. Pre-saturated disposable pads are also available. Similarly, a special lint-free pad is available for cleaning disk heads. Isopropyl alcohol is a safe solvent that can be used to clean heavily soiled heads. These cleaning operations are best performed by qualified personnel; they are presented here only for information. The specified manufacturer procedures should always be followed for each piece of equipment.

Automatic, portable disk pack and disk cartridge cleaning machines are available from specialized manufacturers. These systems can also be used to detect warpage, dents or other damage to the disk surfaces.

Having learned the proper operating and storage techniques, let us review the most important defensive procedures to be observed when using a disk unit.

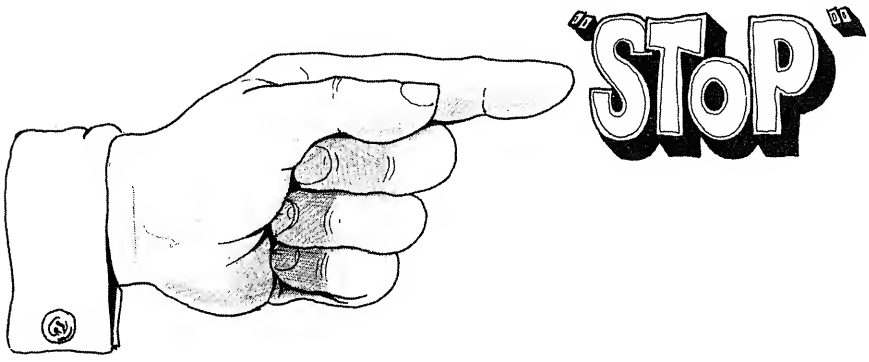
THE MAIN DOs AND DON'Ts—A SUMMARY

Here is a summary of the most important recommendations regarding the proper maintenance of hard disks.

DO

- When bringing a new disk into the computer room, allow the temperature of the disk to equalize with the room temperature for 24 hours before using it. By doing this, you will obtain correct track registration.
- Always handle the disks with great care. Don't drop them. Carry only one disk pack or cartridge at a time. When carrying a disk pack, use the appropriate handles. When carrying a cartridge or a disk pack over a long distance or outside of a building, use a special container.
- Use snap-on covers with front-loading cartridges. Keep disk cartridges enclosed at all times.
- Store your disks securely. Don't store them horizontally unless they fit in a special rack. Stacking disk cartridges is an open invitation to disaster because one of the disks could slip off.
- Keep the computer room dust free and at an even temperature.

- Examine your air filters at least once a week. Replace the disk drive's air filter at least once every six months.
- Always use the correct type of cartridge.



DON'T

- Don't smoke. This is an easy way to cause a head crash. Look at Figure 4.7 and examine the size of a smoke particle compared to the clearance between the head and the disk platter.
- Don't put your fingers or any object on the disk surface.
- Don't play with the power lines or the fuses while the disk is operating. Always turn your disk drive off if you are doing something that could interrupt power to the system.
- Don't turn on any other powerful device while your disk drive is operating. In particular, don't turn on a coffee maker that is connected to the same line as your disk drive. Don't plug a vacuum cleaner into the same outlet either.
- Don't leave the computer room without properly backing-up your disk. Again, at the time a cartridge or a pack is removed from the disk drive, label it completely, including the date. Store it securely.

CHAPTER 5
THE COMPUTER

Awake, arise, or be forever fallen!
— Milton, Paradise Lost, I, 330

FOR THE HOME COMPUTER USER

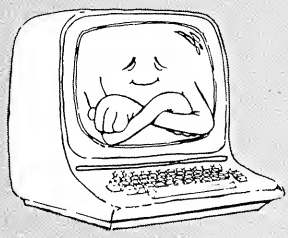
The main rule is:

Avoid electrical interference.

This means two things:

1. Connect your computer to a separate circuit whenever possible. Don't use an outlet connected to the same circuit as an appliance. The line voltage might drop unexpectedly.
2. Avoid static electricity.

Also, if your computer incorporates disk drives, protect it from dust. Use a plastic cover if necessary.



INTRODUCTION

The computer proper is the part of the system that generally requires the least care and maintenance. However, since it may fail or malfunction, it is useful to understand what the main components of the computer are and the proper precautions that should be taken when using it.

UNDERSTANDING YOUR COMPUTER

The computer proper executes programs that process information or data. Both programs and data are generally stored in files residing on tape or on disk. The computer is the processing module of the system. It has four *functional* elements:

1. a *central processing unit (CPU)* that executes the programs
2. the *main memory,* that stores the programs and the data for the central processing unit
3. *input/output (I/O) interfaces,* that are required to communicate with the peripherals
4. a *power supply* that powers the computer.

We will examine these elements in turn.

The CPU

The CPU (Central Processing Unit) executes the programs. It generally resides either on one board or on a part of a board. It uses few components and seldom fails. Most recent CPUs use a microprocessor, plus a few timing circuits. Computers that use a microprocessor as their CPU are called *microcomputers.*

The Memory

The memory stores information. The internal or main memory of the computer uses MOS LSI chips. MOS (Metal Oxide Semiconductor) is the name of the technology used to manufacture the chips, and LSI stands for Large Scale Integration. Each memory chip stores several thousand bits of information (8 bits are used to store one character).

A typical business computer memory has at least 64K bytes (one byte is 8 bits and 1K is 1,024) and resides on one or more boards. The memory uses

many chips and is a likely source of malfunctions. Memory chips, like all MOS chips, are affected by heat and may malfunction at random times when the temperature rises, thus making a diagnosis difficult.

The I/O Interfaces

The input/output interfaces are used to communicate with the peripherals. Interfaces usually occupy one board per function. For example, in a system that uses floppy disks, a floppy disk controller board resides in the computer and provides the required interface between the central processing unit and the disk drive electronics. A hard disk also requires a specific controller board that resides within the main computer enclosure.

Most computers incorporate standard serial and parallel interfaces, so that printers and CRTs may be easily connected to appropriate connectors in the back of the computer cabinet. When these standard interfaces are not provided, an additional serial or parallel communications board is required to connect a printer.

On home computers, a direct *video output* is sometimes provided so that information can be displayed on a television set or on a monitor.

Since interface boards communicate with the central processing unit and the memory, propagation delays must be kept to a minimum. Therefore, the memory must be in close proximity to the central processing unit and the interface boards must reside within or close to the computer enclosure. They are generally plugged directly into the computer's *motherboard,* which is the main computer board into which all others are plugged. Sometimes, a rack equipped with female connectors is used instead of a motherboard. The interconnection path of these boards inside the computer is called the *internal bus.*

Interface boards that use relatively few chips are not likely to fail. Therefore, a *dense* memory board is generally the first suspect in case of a malfunction.

The Power Supply

In addition to the CPU, the memory and the interfaces, the computer proper incorporates a power supply that delivers the required voltages to the boards. The quality of the power supply is a key element of reliable computer operation. We will see that the main cause of disruption to a computer is electrical pollution or noise, coming in through the power line.

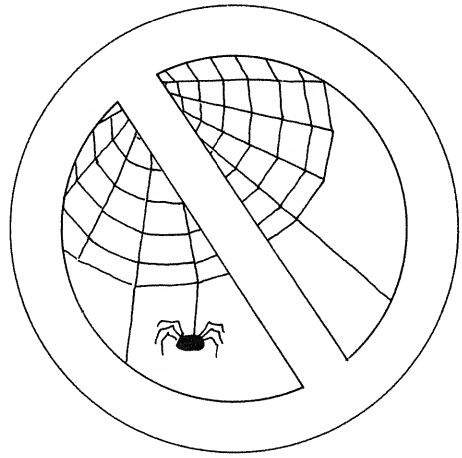
OPERATING THE COMPUTER

All of the components of the computer proper are solid state devices; they have no mechanical parts except for the ON/OFF switch (or key). As a result, they require virtually no maintenance. As long as no one touches the inside of the computer, most failures are normally of an electronic nature, and precautions must be exercised at that level. However, in the event that operators and other users have access to the inside of the computer box, additional mechanical problems may occur.

Let us first examine the proper physical environment and then the electrical environment.

The Physical Environment

Because of their solid-state construction, most mini- and microcomputers are rugged and relatively immune to dust, shocks, and vibrations. They require fewer precautions than disk units. However, problems may still occur if basic precautions are disregarded. We will therefore present the proper procedures and precautions relating to dust, shocks and vibrations, pollution, liquids, and temperature.



Dust

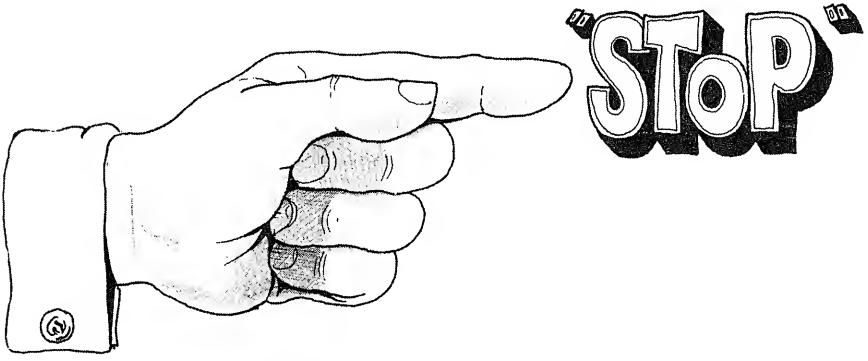
Dust should be carefully removed from ventilation inlets and outlets on the computer. It is good practice to inspect the ventilation outlets on all devices at least once a month. In particular, the fine dust generated by the paper used with a high-speed printer can clog the wire mesh on a ventilation outlet and cause internal overheating. Malfunctions or even a circuit

burnout may result. As a general rule, eliminate sources of dust in the room and check surfaces for dust accumulation.

Shocks and Vibrations

A well-built computer is reasonably immune to shocks and vibrations. However, repeated small shocks or vibrations have a cumulative effect. For example, internal screws holding heavy parts, such as a transformer, may come loose in time. There will be no visible symptom of a problem until the day the computer is moved, and the transformer inside suddenly shifts and crushes or shorts out essential circuits. The damage may then be very substantial.

Vibrations may also dislodge internal boards, causing erratic malfunctions. When a computer is inspected internally after a malfunction has occurred, one of the first rules is to verify that all boards are properly inserted and that all components are properly seated in their sockets.

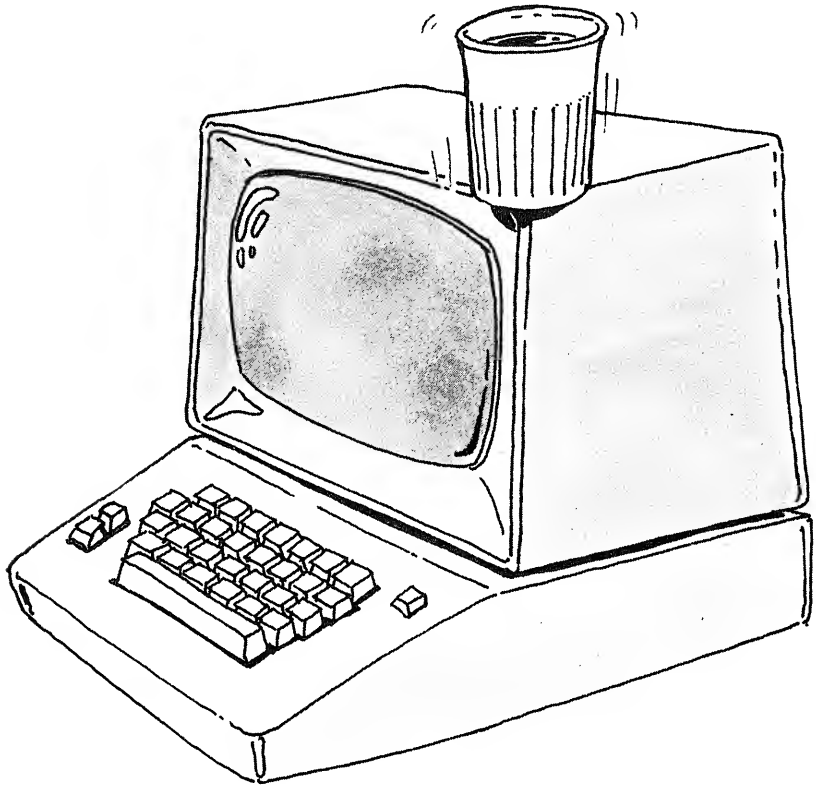


In particular, don't place your computer on the same table as a printer (avoid vibrations), and don't let any part of the computer protrude from the table (avoid shocks).

Pollution

Pollution will corrode the copper contacts of edge connectors and components. If a board or a set of components are stored away from the computer, the contacts should be carefully cleaned before the board or

component is inserted into the computer system. Cleaning the contacts of an edge connector will often eliminate a malfunction. An eraser can be used to clean the contacts of an edge connector—but watch for debris. Similarly, cleaning all of the pins of the components on the board may eliminate a malfunction. A proper solvent should be used for this task. When removing integrated circuits, use a special IC extractor, or you may bend the pins.



Liquids

Liquids spilled on an electrical circuit spell its death. Liquids should be kept away from any electronic boards. They present two dangers:

- First, any liquid will destroy one or more boards inside the computer by shorting out circuits.
- Second, an electrical short may result in a fire or even a minor explosion. It is strongly recommended that you keep all liquids out of the computer room unless the operator is fully aware of the dangers incurred by allowing liquids near electronic equipment.

Here is a horror story.

When a 7600 ("Star") super computer from Control Data Corporation was installed at a well-known university campus, an inauguration party was held. This was one of the fastest commercial computers ever built and one of the most expensive. Incredibly, soft drinks were made available in close proximity to the computer equipment. Predictably, one of the guests put a cup of soft drink on top of the oil-cooled central processing unit cabinet. Subsequently, it was knocked over and spilled. The central processing unit was instantly destroyed. The same result can easily be achieved on a much smaller computer.

The ban against liquids in the computer room also applies to automatic fire-extinguishing systems. Dousing an electrical fire with water is counter-indicated and will cause extensive damage to the equipment, as well as spark additional fires. Whenever possible, alternative fire-extinguishing systems should be used. An automatic sprinkler system can be triggered by a sharp rise in the temperature of a room. If one of the sprinklers in a computer room is triggered, the computer will be lost, and the likelihood of a violent electrical fire will be high. This topic is addressed in Chapter 9.

Temperature

As long as the electronic components used in manufacturing the computer are of high quality and the workmanship of the assembly is good, the computer proper can be the most reliable part of the entire system, and will require the least maintenance.

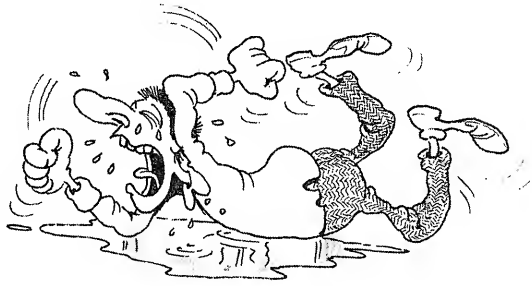
The probability of component failure increases with the number of components in the system and with the temperature. Small computers use few components and are therefore intrinsically very reliable. Unfortunately, the probability of failure also increases very rapidly as the temperature increases. A higher operating temperature will cause marginal components to fail, often in an erratic and hard-to-detect fashion. The temperature of the surrounding environment should therefore be kept as cool as possible in order to prevent random failures.

In addition, at higher temperatures, not only does the probability of computer failure increase very rapidly, but also the life of each component is shortened (this is known as accelerated aging). It is generally thought that a temperature rise of 25°F (14°C) will reduce the life of an electronic component by 50%. The greater the temperature rise, the shorter the equipment life. The recommendation is, therefore, to keep the computer operating in a cool environment whenever possible. Adequate ventilation should be provided and the ventilation openings of the computer box should always be kept free of obstructions. The investment in proper ventilation, preferably an air conditioning system, is usually worth it.

A rise in temperature may be caused by several factors: the weather, inadequate ventilation, a large number of people in the room, several machines operating simultaneously in the same room, and sunlight coming in through the windows. All possible sources of heat should be reduced in order to extend the life of the system and to guarantee reliable operation.

For proper heat dissipation, remember that there should be proper clearance underneath the computer, behind it, and over it—depending on where the ventilation openings are located. Often, air inlets are located underneath the computer box. In that case, the box is elevated, often with rubber pads, to leave a space between the top of the table or desk and the bottom of the computer box. Don't obstruct this space. When air inlets or outlets are located in the back of the computer, leave some space between the computer and the wall. Air outlets are generally on top of the computer and should not be obstructed.

Here is a typical horror story.



A computer cabinet has one set of ventilation slots on top of the cabinet. A careless operator places two diskettes on top of these ventilation slots. Within 5 minutes, the computer starts behaving erratically. The cause of the failure is not readily identified because the computer behaves in a strange way. A hardware failure is suspected. Naturally, by the time the hardware serviceman arrives, the offending diskettes have been moved to their proper location. Thus, no failure occurs. However, a few days later, the problem reappears for no obvious reason. Since the hardware received a clean bill of health, the program is suspected.

At this point, it looks as if the reason for the failure may never be found. The software vendor is first incriminated, and then the hardware supplier. Both deny that any problem exists. Yet the system continues to fail once in a while without anyone understanding why. The reason for the failure is the faulty handling of the diskettes by an operator. However, once the operator replaces the diskettes in their proper containers and leaves the room, there is no longer any proof of the offense and no one is be able to diagnose the problem.

Physical Environment Summary

Keep your computer operating in a cool environment. The greatest danger to a computer can come from the inadvertent blocking of ventilation openings which may cause overheating and thus erratic failures. Although they are not frequent sources of problems, condensation, dust, shocks and vibrations should also be avoided.

Let us now discuss the computer's electrical environment and examine the computer's other great enemy: disruption in the power line.

The Electrical Environment

A computer must have a clean and stable power supply. Anything interfering with the supply of a completely stable voltage to a computer will

disrupt its operation and cause failures that are hard to diagnose.

We will first examine the power requirements of the computer, then we will look at the common causes of disruption, along with some remedies.

Power Requirements

A computer executes a sequence of instructions called a program. Each instruction is executed in about 1 microsecond (1 microsecond is one millionth of a second). The elementary operations required to execute an instruction occur in a few tens of nanoseconds (a nanosecond is one thousandth of a microsecond). Because of the very high speed at which a computer operates, it cannot tolerate any variation in the electrical power that it receives.

All computers are equipped with a power supply that transforms the line voltage (110V at 60 hertz or 220V at 50 hertz) into the voltages required by the various components inside the computer. For example, a typical power supply may internally deliver + 5 volts, + 12 volts, and − 12 volts DC from an external 117V AC line. Most power supplies will accept voltages within a plus or minus 10% range of the nominal value. For example, a power supply rated for 117 volts, plus or minus 10%, will accept an input voltage ranging from 106 to 128 volts. However, these are the extreme values that the power supply will accept. If the voltage should rise or drop by several volts beyond the tolerance levels, the power supply will no longer be able to deliver the guaranteed voltages, and the computer will malfunction. Similarly, the frequency of the line must usually be guaranteed within 1 hertz. In particular, a computer rated for 60 hertz will normally not function on a 50 hertz power line. Since a large number of computers are manufactured in the United States and are used in other countries, a problem arises because a 60 hertz frequency is used in the U.S., and 50 hertz is used throughout most of the rest of the world. In order to be usable overseas, a U.S. computer must be rated for 50 to 60 hertz or, preferably, for 47 to 63 hertz.

The internal power supply of a computer system is one of the more expensive components of a system. As a result of its higher cost, the better computers have a higher quality power supply that can smooth out temporary variations (fluctuations) of the power line. However, the majority of computers have a less expensive type of power supply which will tolerate only minor, slow variations in the line voltage.

Unfortunately, the power delivered by most electrical companies is neither stable nor accurate. Furthermore, even when the power is reasonably

accurate most of the day, it may suddenly become unacceptable for proper computer operation at other times. Every user of a business or scientific system should be aware of these possible variations throughout the day.

It is essential that a stable, fixed voltage be supplied to a computer. In general, the nominal voltage in the U.S. is 117 volts. However, the actual voltage varies with the distance from the power station and the load on the line. It may go as high as 130 volts and as low as 100 volts. Most transformers used in power supplies are equipped with straps so that they may be set to several input voltages, for example: 100, 110, 120 and 140 volts.

To insure the reliable operation of a computer system, the first step to take when installing it is to periodically check the value of the line voltage throughout a typical day. An ordinary voltmeter can be used. Make sure that the line voltage matches the setting of your computer power supply, and that it does not vary by more than 5% throughout the day.

In order to prevent interference with the line voltage, the computer system should operate on its own electrical circuit, connected directly to the main distribution board of the building. No other devices should be connected to the line that supplies power to the computer and its peripherals. In some cases, powerful peripherals, such as hard disk drives or high speed printers, may also require a dedicated power line. If such devices are connected to the same line as the computer, they should not be turned on or off while the computer is operating.

Let's look at a simple procedure for avoiding possible power line interference:

1. Use a dedicated circuit for the computer.
2. Periodically measure the line voltage throughout the day.
3. While the computer is running, turn on and off all major appliances, such as air conditioners, heaters, office copiers, and other large machines in the building, and verify that they do not interfere with the proper operation of the computer.
4. While the computer is running, turn on and off all electrical devices in the computer room and verify that they do not interfere with proper computer operation.
5. Pull the circuit breaker for the computer system at the main distribution board, and make sure that nothing else in the building is turned off by this action; but first, be sure to remove disks from disk drives and to properly prepare the computer for a power failure.

It would also be wise to put a notice on the main electrical distribution board, warning people not to tamper with the computer circuit or the ground wire without first notifying the computer operator.

This should be done because if there is an electrical problem in another part of the building, someone will most likely open the main distribution panel in order to replace a fuse or check the circuits. If the computer circuit is not clearly identified, power to the computer system may be inadvertently disrupted, causing a serious malfunction, especially if a disk is being used. In the event the computer circuit or the ground lines must be

tampered with, the computer operator should be notified so that the disk units can be stopped, any diskettes removed, and the computer system properly shut down.

Finally, a business-type computer requires two grounds: a *reference ground* and a *safety ground*. The reference ground is a third isolated wire. (This requirement will be explained in Chapter 9.) The safety ground is for personnel safety. It is connected to all chassis.

The green wire carries no current unless a malfunction occurs in equipment connected to it, or lightning strikes. It also provides operator protection against static. In the U.S., it is generally green, sometimes yellow.

The reference wire minimizes electrical noise and carries a current. It is generally white.

In summary, the three main electrical requirements are:

1. sufficient voltage
2. clean power
3. proper grounding.

Two important consequences are, therefore:

1. Use a dedicated circuit.
2. Provide two grounds.

Let us now examine the possible problems that can affect the electrical environment and their solutions.

Electrical Problems

Six main types of electrical problems may be encountered:

1. *fluctuations,* which are slow variations of the electrical power
2. *line transients,* which are fast temporary variations of the line voltage
3. *electromagnetic interference (EMI),* which may disrupt both the external power supply and the signals inside the computer
4. *brownouts,* which are voltage reductions planned by the power company
5. *power failures,* which are unplanned interruptions of power
6. *static electricity,* which builds up in a dry environment.

We will examine each of these electrical problems in turn.

Fluctuations. Fluctuations are defined as slow variations of the line voltage (over many cycles of the sine wave). Fluctuations are characterized by a *sag* (voltage too low) or a *surge* (voltage too high) in the line voltage. They result from dynamic loads on the line, which can be caused by motors and certain appliances.

Fluctuations are normally corrected by the power supply. Whenever fluctuations exceed the limits of the power supply tolerances, they may be corrected by using an inexpensive power *line filter* (see Figure 5.1). A line filter will remove short-lived fluctuations. However, it will not correct a brownout where voltage remains too low over a long period of time. A *line conditioner* will then be required.

Line Transients. Line transients are fast changes in the power line that occur in a few cycles or less (typically in microseconds). A transient voltage drop is called a *notch* or dip. A transient voltage increase is called a *spike* or sometimes a *surge*. Transients are usually due to electromagnetic causes. They may be due to lightning, inductive kick-back, or electromagnetic radiation (EMI). Inductive kick-back can result when motors and

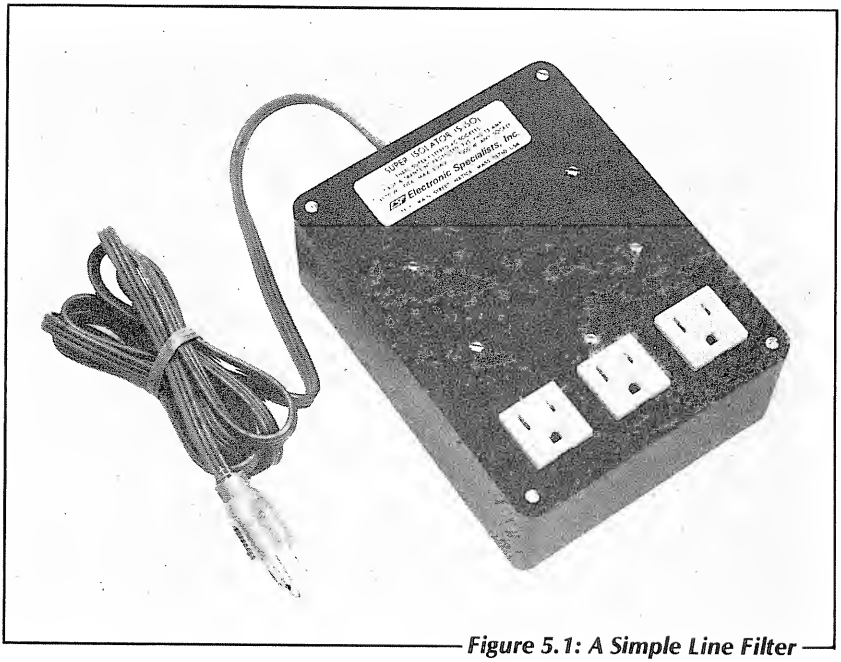


Figure 5.1: A Simple Line Filter

other equipment connected to the power line are turned on or off. Sources of EMI include car ignitions, overhead fluorescent lamps, appliances, radio or TV transmitters, radar equipment, as well as any powerful machine used in the medical or industrial environment that emits electromagnetic radiations.

Inexpensive power supplies used in low-cost computers offer little protection against such line transients. Higher quality power supplies used in larger business computers usually incorporate filters designed to remove or limit the effect of transients.

Series of transients are a form of *noise*. Noise refers to all disruptions of useful signals, both on the power line and inside the computer, and is the primary effect of EMI.

If your computer is affected by transients and noise, two approaches are possible:

1. If the source of the transient or the noise can be found, it should be removed. Whenever possible, any source of noise or interference should be removed, even if a good power supply is available, since noise may affect not just the line voltage but also the internal signals propagated inside and outside the computer itself. This applies, in particular, to CB radio transmitters and to any improperly shielded machinery that emits electromagnetic radiation.

2. An inexpensive *line isolator* (or isolation transformer) may be used to filter out most common types of transients. A line isolator incorporates a transformer and typically filters out common voltage spikes or short-lived dropouts in line voltage.

It is recommended that you use a separate isolator for each large piece of equipment. For example, one line isolator may be used for the computer and perhaps the disk drive, while another isolator is used for the printer and the CRT display. Typically, such isolators include *low pass filters* that will also eliminate noise, such as the noise created by a radio transmitter nearby. Because they are inexpensive, the use of isolators is recommended in all cases where the computer power supply does not already provide this function.

In cases where all of the above problems occur together, a *power conditioner* must be used. This is a more expensive device that both regulates and isolates the line, delivering a guaranteed voltage level at its output. A good power conditioner will cut out virtually any noise or signal to a very small fraction of its value (less than one millionth).

Spikes or surges are a special case of line transient and deserve special attention.

Surges: Surges (high voltages) can be caused by lightning, a power outage or restoration, heavy machinery, and air conditioners. If the surge is powerful enough, an arc will occur across OFF switch contacts, or between contacts and ground, even though the equipment is off. Such an arc can destroy transformers and electronic components.

Most good power supplies will incorporate some type of surge protection. If yours does not, then surge protection can be obtained by purchasing an inexpensive *surge protector* or a line isolator with surge protection.

If a blackout occurs in your building, turn all equipment off and, if possible, pull plugs out of their sockets. Surges are likely when power is restored and they could blow equipment fuses or damage components.

Electromagnetic Interference. EMI (electromagnetic interference) designates all of the spurious signals generated by electromagnetic radiation, throughout the computer system and the cables attached to it. Line transients are just one of the effects of EMI.

Interference with the electrical or the electronic operation of a computer may occur in the following locations:

1. *Outside the computer room.* Interference may affect the power being delivered to the computer. Depending on their duration, these variations in the line voltage are called line fluctuations or transients and have already been described.
2. *Inside the computer room, on the power line.* Electromagnetic interference may induce electrical phenomena throughout the computer, including the power line. Its effect is induced noise.
3. *Inside the computer room on signal cables.* Electromagnetic interference may affect signals traveling in cables outside the computer. This is also an induced noise problem external to the computer itself.

Recall that EMI may be caused by communication equipment (radio, television, radar); electrical tools; an electrical arc (arc welders, static sparks, thunderstorms); car ignition systems; appliances (vacuum cleaner); power lines and business machines. Two types of EMI are distinguished:

1. *Common Mode EMI*, when noise exists on the hot and the neutral wires and not on the green (safety ground) wire. Filters must be installed between hot and green, and neutral and green.
2. *Differential Mode EMI*, when noise exists between the hot and the neutral wire, and generally only on one of them, not both. A filter must be installed between hot and neutral.

Since both types of EMI may be present, filters are installed between all of the above pairs of wires.

We have already seen that the common effects of EMI can be reduced or removed from the power line by the use of a line isolator (isolation transformer). However, the computer and the cables themselves may be a source of EMI. In particular, interconnection cables should be kept short and away from the power line. Transients traveling along the power cable may be stopped by the computer power supply or by the line regulator. However, if this cable is in close proximity to connection cables such as the cable between a disk drive and the computer, such transients may induce noise in that communication cable and cause failures to occur. Also, avoid running interconnection cables close to powerful sources of electromagnetic radiation such as the left side of a color television or monitor, or the power supply of a device, or even a telephone set.

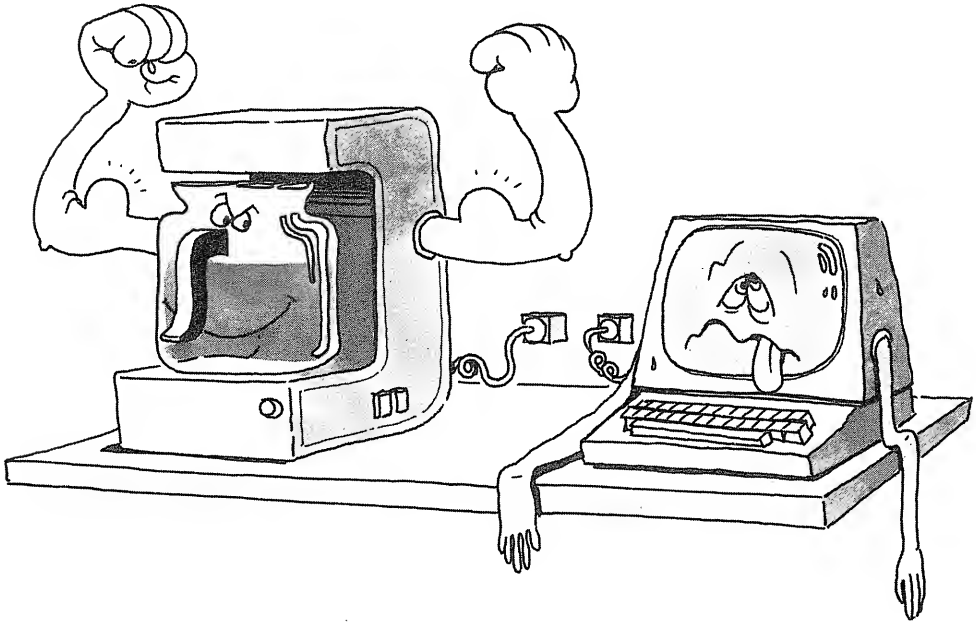
Always leave covers and shields in place. All large metal surfaces should be grounded, including window screens. All magnetic media should be stored in closed metal cabinets for their protection. Finally, avoid dimmer switches in the computer room, as they generate EMI.

Here is a checklist of common sources of noise or "hash":

- lightning
- motors
- fluorescent lamps
- arc welders
- diathermy machines
- computers
- printers
- disk drives
- electrical tools
- appliances
- automatic door openers
- electrical display signs
- elevators/escalators
- pumps, fans
- noisy electrical sockets, plugs, and wiring (when loose, defective or corroded)

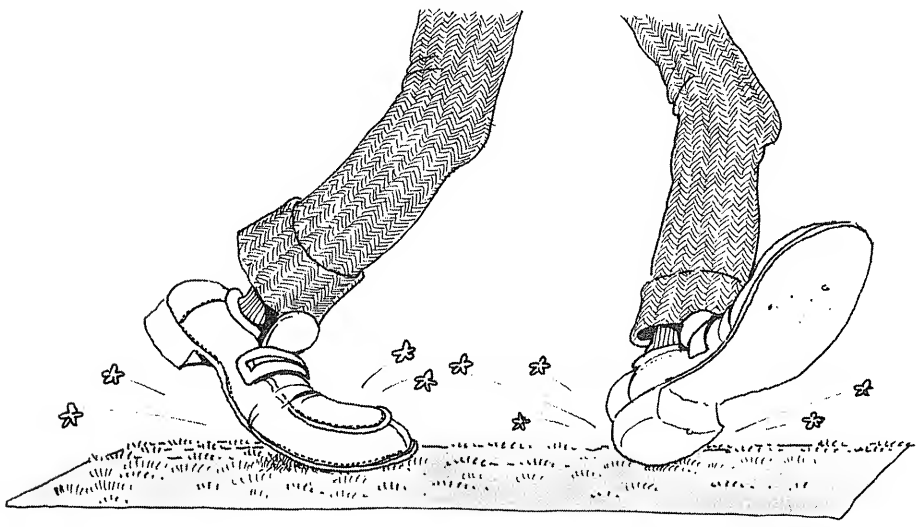
Brownouts. In some areas of the country, "brownouts" are common during periods of heavy electrical use. During a brownout, the power company deliberately reduces the line voltage to avoid an overload situation. When this occurs, the voltage may drop by 8% (or even more). This drop will cause a computer failure. When brownouts are a problem, *power conditioners* must be used to restore sufficient voltage.

Short-lived brownouts can also be caused by switching on a powerful device that is connected to the same power line as your computer. This may occur within the computer room itself (for example, when a coffee pot is turned on), within the building itself (for example, when a vacuum cleaner is turned on), or sometimes because a large machine is turned on in a nearby building connected to the same power line. The flickering of the lights in the computer room is an obvious indication that a short duration brownout has occurred. Even a short-lived brownout will cause a computer malfunction.



Power Failures. If power is interrupted for more than a very few milliseconds (one ms is one thousandth of a second), the computer will fail. Most good computer systems are equipped with a power failure detection circuit that will alert the processor to this event. When the voltage drops below a certain threshold, a power failure routine is activated that preserves as much of the state of the system as possible in order to allow an orderly shut-down. In particular, the disk drive is deactivated, and the disk heads are lifted in order to prevent a head crash. Any program that was in execution at the time that the power failed is stopped and the files that it was handling may be left in an indefinite state although not necessarily damaged.

If short power failures (of a few milliseconds or seconds) are common in your area, they can be remedied by using a *battery backup.* However, a battery backup is generally very expensive and its cost rises very rapidly with the length of time that it must deliver power. It represents a practical solution only in cases where the power is interrupted for a very short time. It is also possible to use a *motor generator* for interruptions lasting from 200 microseconds to several seconds. When power is interrupted for a longer period of time (say minutes), the cost of a battery backup generally makes it impractical.



Static. Interference with proper computer operation may also be caused by static electricity. Static electricity will disrupt the operation of any electronic component. On a dry day, 10 steps on a nylon rug can build up from 10,000 to 20,000 volts of static electricity in the body. By simply rising from a chair insulated from the floor (rubber casters), you can generate 10,000 volts. If you build up the voltage and point a finger at a component or a board you may "french fry" the component, i.e., cause its immediate destruction with a static electricity discharge. Touching a key on the keyboard, the frame or any peripheral of the computer, will cause a sufficient discharge to disrupt the computer's operation or even damage the computer permanently. Static electricity is a serious danger for any computer installation and should be carefully avoided.

We have examined all common electrical and environmental problems along with recommended procedures and precautions. We will now review the equipment available to correct these problems.

Equipment Review

Four types of equipment are available to correct line and noise problems:

1. isolation transformers
2. regulators
3. line conditioners
4. uninterruptible power systems (UPS).

We will examine each in turn.

Isolation Transformers. An isolation transformer attenuates voltage variations between primary and secondary windings, thus attenuating short transients (spikes) and high frequency noise. Isolation transformers are generally used as inexpensive line filters.

A *super-isolation transformer* uses a shielding technique on the windings to further reduce common-mode voltages between the windings. It is typically 1000 times more effective than a plain isolation transformer, providing over 100 db common-mode rejection, as well as transverse noise rejection. This type of transformer does not, however, correct slow line voltage changes such as brownouts. A super-isolation transformer is shown in Figure 5.2.

Regulators. A regulator maintains a constant output voltage, despite variations in input line voltage. It protects against slow voltage variations, including moderate surges and brownouts. Many regulators have auto-transformers and provide no transverse noise rejection.

Line Conditioners. A line conditioner is a regulator that includes an isolation transformer. The terms regulator and conditioner are sometimes used interchangeably. A line conditioner provides voltage regulation and noise rejection. A portable ultra-isolated regulator is shown in Figure 5.3 and a larger line conditioner (3 kVA) is shown in Figure 5.4.

Uninterruptible Power Systems. A UPS provides power continuously, even when the AC power is interrupted. In addition, it filters noise.

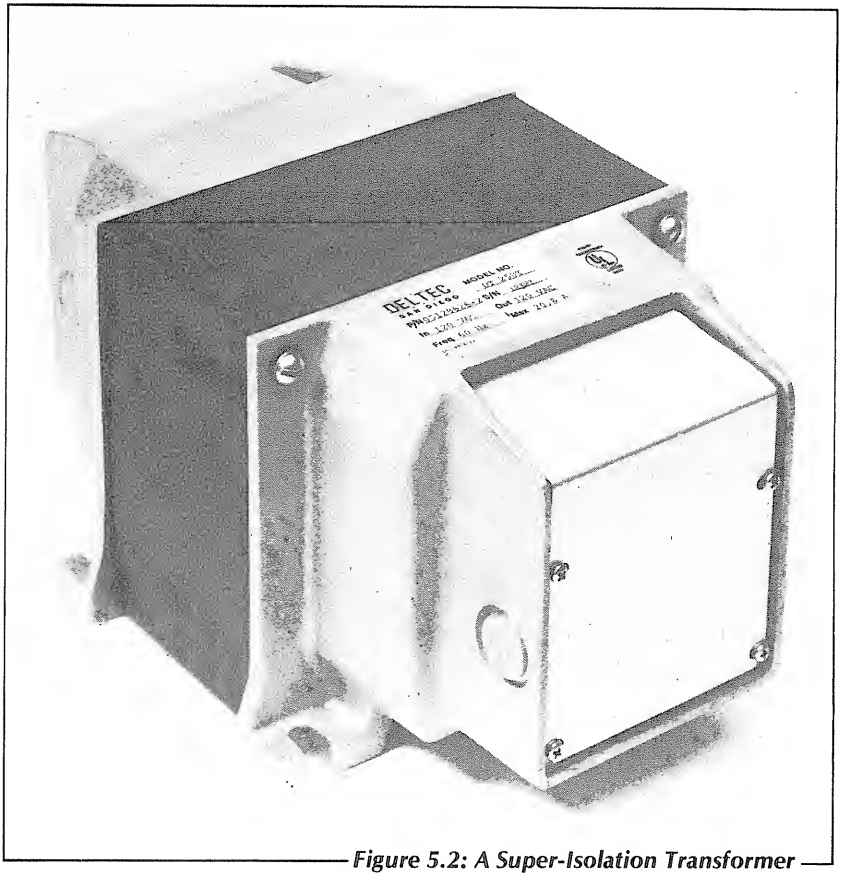


Figure 5.2: A Super-Isolation Transformer

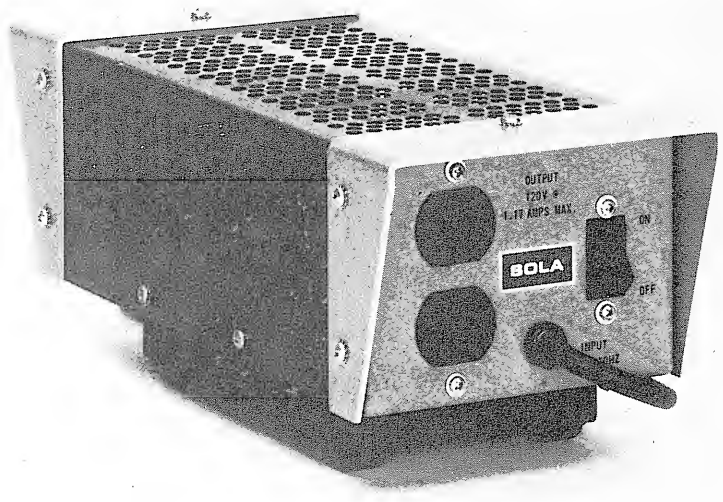


Figure 5.3: A Portable Ultra-isolated Regulator

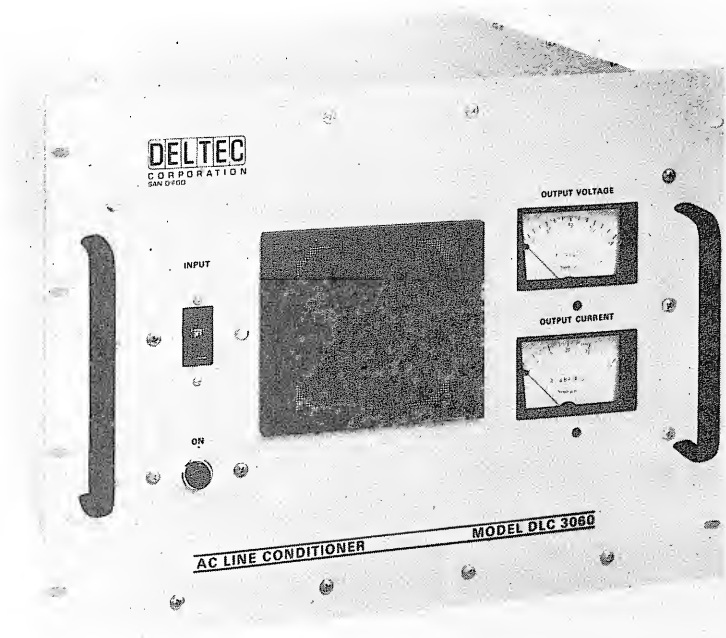


Figure 5.4: A Line Conditioner

It is the best but most expensive solution. A UPS includes a rectifier/charger, a battery and an inverter. The charger is connected to the AC line and charges the battery. It includes a filter against transients. The DC to AC inverter provides power to the computer system from the battery. A UPS is shown in Figure 5.5.
Now that we have described all common problems and remedies, we will present additional recommendations for the dedicated tinkerer.

INSIDE THE COMPUTER

You are not supposed to open your computer. However, at times, it may be necessary to open the cover of the computer in order to inspect the boards or to replace them. The main recommendation is: don't do anything inside the computer unless you know what you are doing. Naturally, if you open the cover, the power should be off and the power lines should be unplugged from the outlet.

Many computer boards, such as memory and I/O boards, are equipped with micro-switches, generally located close to the edge of the board. These switches are used to select or to specify options or addresses needed by the system. Inadvertently touching one of these switches will prevent proper system operation. If you plan on accessing the inside of your computer, it is highly recommended that you write down the proper switch positions of each board in a computer log book or reference manual. This will enable you to verify the proper settings prior to closing the computer cover.

When you open the computer, first remove any visible dust accumulation. A can of compressed air can be used. Be careful not to dislodge a board from its socket. By pushing a board sideways, you may produce incorrect system operation, paralyze the entire system, or create a short that will burn out the power supply as well as one or more of the boards.

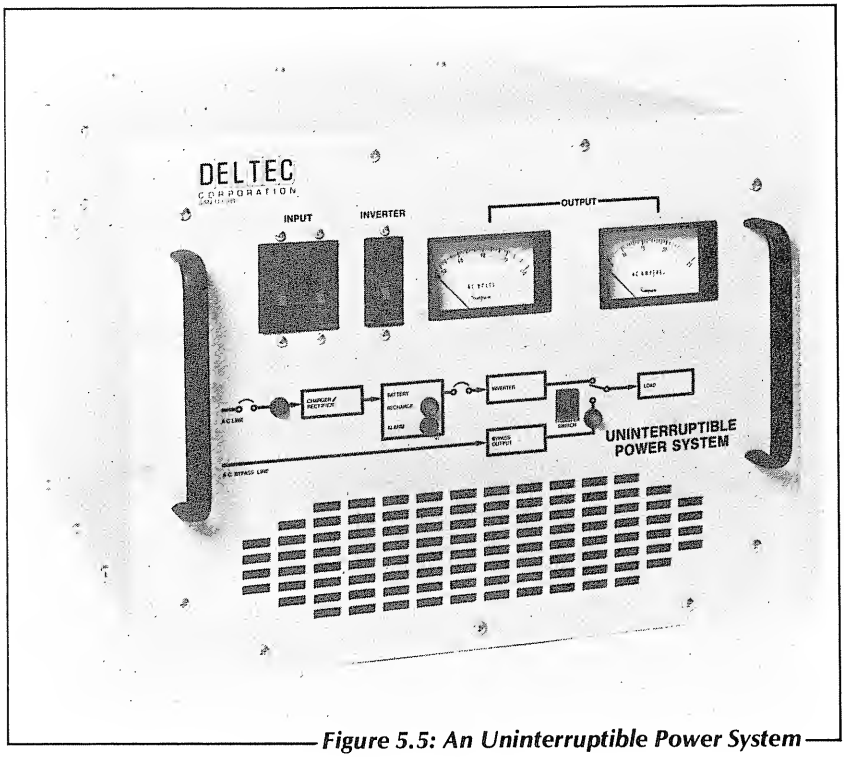


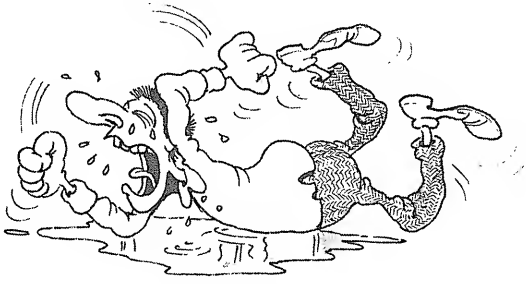
Figure 5.5: An Uninterruptible Power System

When working inside the computer system, be careful not to drop any conductive object such as a staple, paper clip or any liquid into the computer. Before closing the computer, it is a good idea to gently tilt it and watch for loose objects such as screws or debris that might impair its proper operation.

Finally, inspect the points at which cables are attached and make sure that the connections are secure. External cables should not be allowed to pull directly on an internal system component. Some kind of mechanical safeguard should always be used so that if someone accidentally or deliberately pulls on an external cable, none of the internal components connected to that cable will be dislodged. This can sometimes be achieved by merely tying a knot with the cable inside the enclosure. Preferably, a special connector should be installed within and attached to the enclosure so that pulling an external cable will not result in an adverse effect inside the computer enclosure.

Many interface boards for microcomputers (such as serial interface boards) are sold for direct insertion into an S-100 connector—a common standardized connector inside many computers. A serial board allows the computer to communicate with serial devices, such as a CRT or printer. The board must be inserted into the proper computer slot and a cable must be attached to it. The proper way of doing that is to solder one end of a cable to the board, and the other end to a proper female connector that may already exist or that must be installed on the back of the computer enclosure. However, many first-time users simply attach the cable directly to the board. Letting it run through one of the openings in the back of the cabinet, they then connect the other end of the cable to the peripheral device.

Here is a typical horror story.



Computer System X was equipped with an S-100 compatible serial interface board. It was attached to a brand new printer via a cable. The system operated properly for several weeks. Then, mysteriously, the printer started skipping lines and characters. Failure occurred in a semi-random manner and there was no visible pattern. The printer was carefully checked out and then tried with

another computer. It worked perfectly. The obvious conclusion was that the communications software was at fault. The software was carefully analyzed. Obviously, there was some error in the software design—probably some subtle error.

For days and weeks, the software was examined in detail, rewritten and checked out. The interface board was physically examined and it checked out perfectly. The problem disappeared for a while and then reappeared. The random failures continued. Since it was essential to have clean and complete print-outs, the entire system became useless and was abandoned.

One day, an ingenious person took a look at the serial interface board. Examining the connection of the cable with the board, this person found that the contact on the board had been bent by pulling the external cable, since the external cable was directly soldered to the board itself. As a result, two of the pins were almost touching each other. A slight pressure on the cable, or a variation in temperature, would short out the two pins. The contact was so slight that the problem would occur for a while and then it would disappear. The pins were straightened out and the system behaved perfectly. Naturally, the next step was to install a proper separate connector on the enclosure that would prevent someone from pulling the external cable and thus bending the pins on the interface board.

COMPUTER SUMMARY

The computer should be properly installed, with adequate ventilation and clean power. The temperature of the room should be kept as low as possible to avoid premature aging. The computer system should be connected to a dedicated circuit, and a thorough check of the line voltage level should be made at the time of installation. If necessary, a line regulator or a line isolator should be used.

All of the cables and connections should be secure. Ideally, all cables should be secured in a fixed position inside the cabinetry or inside the room. Cables should be laid out so that electromagnetic interference will be avoided. While the computer system is being used, all obvious sources of electromagnetic interference should be removed.

Most of the precautions outlined in this chapter are aimed at eliminating transient malfunctions. These are the most difficult problems to detect and correct. Unfortunately, some of the recommendations given may seem superfluous to readers who have not yet experienced erratic behavior.

Remember that if the computer is only used during certain times of the day, and if it has a good power supply, it may operate for months at a time

without a visible malfunction. However, as soon as one of the major environmental conditions changes (for example, if the power supply is disrupted by plugging a coffee maker or a copy machine into the same circuit), then strange problems may start to occur. A precise diagnosis will be difficult if the environmental and electrical requirements are not understood.

In short, it is important for you to be aware of the requirements of your computer system. Then, if you wish, you may decide to ignore some of these requirements until you discover a need for them.

If you take the time now to insure a stable power delivery to your computer, and if you take a few simple precautions to insure a low operating temperature, a clean environment, and a good system installation, you will probably enjoy months or years of trouble-free operation. Further, in the event of a malfunction, you may be able to diagnose the cause quickly.

As a final word, more recently-designed computers will operate with minimal precautions. These detailed recommendations have been presented so that you understand possible dangers in the event they ever affect your computer.

CHAPTER 6
THE CRT TERMINAL

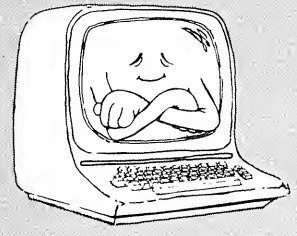
Errors are not in the art but in the artificers.
— Isaac Newton, Principia Mathematica, Preface

FOR THE HOME COMPUTER USER

The CRT terminal imposes no difficult requirements, such as a dust-free environment or very clean electrical power, and it requires almost no maintenance. In fact, neglecting the CRT usually has no visible adverse impact.

The main recommendation is:

Position the CRT for best comfort.



INTRODUCTION

The CRT terminal integrates a keyboard and a cathode-ray tube (CRT) within a single enclosure. It is used to send information to the computer via the keyboard, and to receive information on the CRT display. A typical CRT is shown in Figure 6.1.

In 1965 IBM introduced the first CRT terminal, the 2260. The CRT terminal has slowly, but irresistibly, become the main peripheral for communicating with the computer. It is fast and silent, as well as convenient to use when properly installed and adjusted.

The technical maintenance requirements of a CRT terminal (or CRT) are minimal. They can be summarized by:

Keep it clean and properly adjusted.

The most important recommendations regarding the CRT are aimed at improving working conditions for the CRT operator. In this chapter, we will

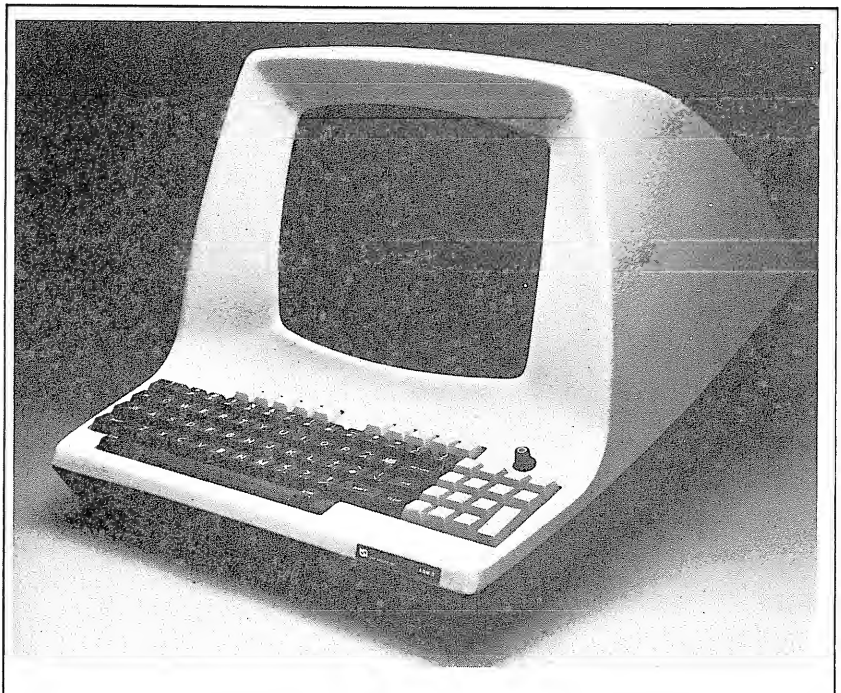


Figure 6.1: A Typical CRT

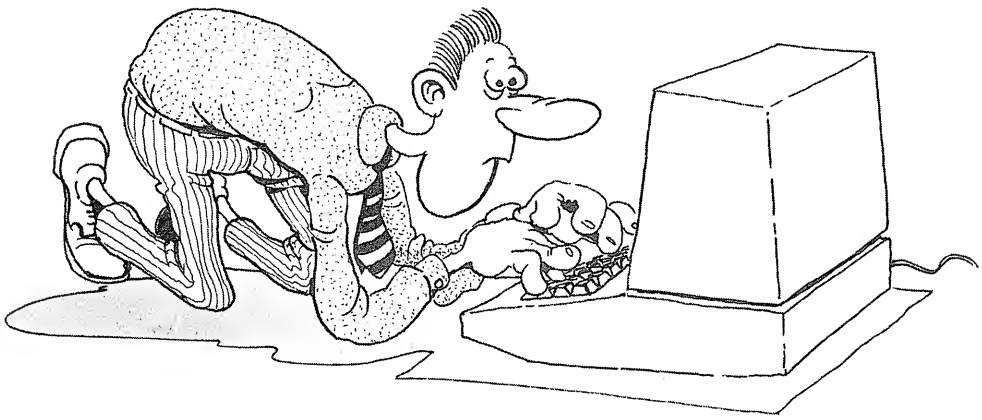
first examine the proper operator working environment and then examine the environmental requirements of the CRT. We will present practical recommendations for the effective use of the CRT and examine two related devices, the CRT monitor and a standard television set.

THE OPERATOR'S WORKING ENVIRONMENT

The CRT is usually the device with which the user of a computer system spends the most time. Proper lighting and equipment positioning are, therefore, essential for operator comfort and efficiency. Let us examine these two factors in turn.

Proper Lighting

The brightness of the CRT screen should be adjusted to a comfortable level for the operator, using the corresponding CRT control knob. In addition, the CRT terminal should be turned away from major light sources (such as windows and fixtures) in order to avoid glare and reflections. Antiglare screens can be installed on most CRTs to eliminate reflections and reduce screen scintillation, thus enhancing readability.



Proper Positioning

The CRT terminal should be installed for convenient viewing and typing. It may be installed on a desk, table, special stand, or pedestal. Proper height is essential for user comfort.

A CRT screen stand is usually lower than a regular desk. A standard sit-down stand is typically 25" to 26" high while a stand-up pedestal is typically 37" to 39" high. A CRT stand generally has a U-shaped base which does not obstruct the legs or the feet of the operator.

For user comfort, the keyboard of a CRT should be placed at a level that is lower than that of a conventional desk or table. An adjustable chair with a proper back is also necessary for operator comfort. The combination of chair and keyboard heights should be carefully selected and adjusted. The position of the operator's arms is crucial to operator comfort. Needless operator fatigue can result from improper height selection. In view of the time spent at a CRT terminal, it is worth adjusting the viewing angle and the positioning of the CRT terminal carefully.

When planning a work station, be sure that there is an adequate working surface available on at least one side of the terminal. This space can be used for the material that is being typed into the computer system. The operator should position the material so that it is either lying flat on the work surface or is being held by a vertical copy holder.

In cases where the CRT terminal is located close to the computer and the room is carpeted or presents a risk of static electricity, the use of an anti-static mat may be advisable in order to protect the computer.

Also, in cases where the operator must move across the room, a swivel base may be used underneath the CRT terminal which will allow the operator to conveniently rotate the terminal. Swivel bases are also useful if two or more operators with adjoining work stations share the same CRT, and if the CRT must be repositioned during certain times of the day in order to avoid sun-glare.

ENVIRONMENTAL REQUIREMENTS

Let us first distinguish between two types of CRTs: the plain CRT, or "dumb" terminal, and the "intelligent" terminal.

The *dumb,* or *plain terminal* simply provides communication capability with the computer via the keyboard and the screen. Most terminals are plain terminals; they are simply used to communicate with the computer and do not perform any local processing.

The more expensive *intelligent terminals* are equipped with a microprocessor and a memory and can do off-line processing of text or information. They can be used, for example, to enter one or more pages of text, verify data entry, and do local editing (text processing) before transmission to the computer. Because of their higher price, they are generally used only with large computers.

Dumb terminals have minimal electrical requirements. They will generally be satisfied with the power provided by the local power company. Disruptions in the power supply are not important since the information is provided directly by the user or the computer itself, and can be regenerated or retyped. Intelligent CRTs, however, are equipped with their own processor and have the same power requirements as a computer, i.e., they require clean power. Disrupting an intelligent CRT is more damaging than disrupting a dumb terminal, since the intelligent CRT processes information that could be lost.

The CRT terminal is almost completely electronic, except for the keyboard, and therefore requires minimum maintenance. The only maintenance requirements are to keep the screen clean for good vision and to keep the keys dust-free in order to insure good contacts and to prevent dust accumulation on the printed circuit board underneath the keyboard.

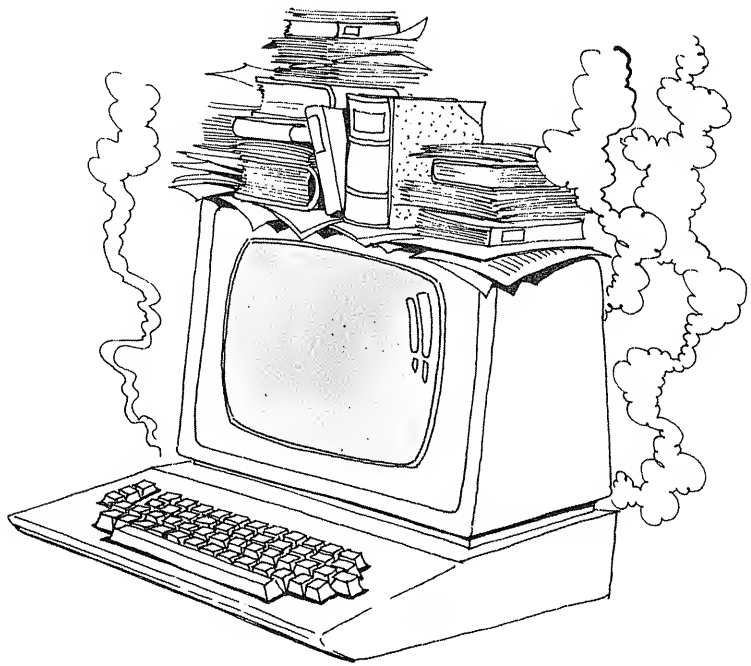
The screen should be wiped clean with lint-free material. If the CRT is equipped with an anti-glare screen, the use of solvents or cleaners is generally prohibited. The outside of the CRT terminal can be cleaned with water and a mild detergent or with appropriate cleaning fluids. Strong detergents and solvents should not be used.

The keyboard is best dusted by using compressed inert gas which comes in a pressurized can. Such dusters are available from computer supply houses as well as photographic stores. Alternatively, a vacuum cleaner with a small brush attachment may be used to clean the keyboard. Neither sprays nor liquids should be used on the keyboard because a drop of liquid might fall on the electrical circuits underneath the keyboard and damage them.

If, by accident, a metal object or any liquid gets inside the CRT terminal, do not use the terminal. Immediately turn it off, and call a qualified maintenance person.

Naturally, shocks and vibrations should be avoided as they may dislodge screws or even the power supply inside the CRT terminal.

Finally, in order to prevent overheating, make sure that the air intake and exhaust slots or louvers of the terminal are never obstructed.



In summary, maintenance requirements for a CRT terminal are minimal. Typically, a good quality terminal that is properly handled will last for years without any additional service or maintenance other than exterior cleaning.

USING THE CRT

There are two main recommendations for using the terminal: know the proper settings, and know the functions of the keys on the CRT terminal. These recommendations will now be presented.

Setting The Controls

Most CRTs allow the user to specify a number of options via knobs and switches. CRTs that are manufactured by independent suppliers are designed to work with a number of different computer systems. They are equipped with switches that allow the user to select an operating mode that is compatible with the specific computer being used. However, CRT terminals that are manufactured by computer vendors usually have fewer manual controls because they are designed to work with only one specific computer. The operating mode is generally under the control of the computer to which it is attached, rather than the control of the user. We will discuss setting the controls for general-purpose CRTs that are manufactured by independent suppliers and that are equipped with the usual options.

A proper setting of the switches is required for correct operation of the CRT terminal. Some switches are designed for operator convenience and efficiency. Although they will not prevent the CRT from operating, they are important to the user and should therefore be well understood. Other switches specify operating options that make the CRT compatible with the computer or printer being used. If one of these switches is in the wrong position, the CRT terminal may not operate correctly.

Screen Brightness

In terms of operator comfort, the most important setting is *screen brightness*. All CRTs allow the operator to adjust the screen brightness to the desired level. In addition, some CRT terminals allow the user to specify *reverse video*, where characters are shown in dark against a bright background. Usually, normal video is used so that the screen is dark and the characters appear as bright adjacent dots on the screen. Use the lowest level of brightness that is comfortable for your eyes.

The Baud Rate

Most CRT terminals are designed to operate from 110 baud to 9600 baud, and some operate at 19,200 baud. In the binary world, a baud is equivalent to a bit per second (bps). The higher the baud rate, the higher the transmission speed of data between the CRT terminal and the computer. You should use the highest baud setting that your computer will accommodate. The highest transmission speed is generally determined by the communications software rather than by the computer itself. However, in some cases, the maximum speed is limited by the communications interface used. Check to see that you are using the highest baud rate possible, i.e., 19,200 baud if available, or if not, 9,600 baud. Your CRT will operate without malfunctioning at a speed slower than the maximum possible, but you will be wasting much time waiting for your output to appear on the screen.

Here is a horror story that will remind you to check the speed setting on your CRT.

In order to obtain listings (printouts) of the information shown on the screen, a printer is sometimes attached to the back of the CRT terminal. (The process is explained below.) In one case, a user attached a 300 baud Decwriter, a slow printer, to the back of a CRT terminal. The baud rate of the CRT terminal was set to 300 baud—the low speed required by the printer. When the usual computer operator later returned to the CRT, the printer had been removed. However, the baud rate switch on the CRT had not been returned to its normal setting and remained in the 300 baud position.

The regular operator initially noticed that the CRT terminal was rather slow but then simply forgot that the terminal had ever been faster. As a result, the CRT terminal operated at very low speed over a period of several days until someone finally noticed that the speed setting was wrong and reset it to 19,200 baud, a speed improvement of 60 times.

When changing the baud rate of the CRT, don't forget that the computer must be informed of the higher transmission rate that has been selected. Often this requires restarting the computer.

The Other Switches

In normal use, the other switches on the CRT terminal should not be changed. It is recommended that the proper switch settings on the terminal be recorded in the computer log or posted on a bulletin board so that the switch positions can be inspected at a glance to insure correctness. Let us now briefly examine the function of the other usual switch settings on a typical CRT terminal.

Parity. When transmitting a byte (8 bits) of information, the eighth bit may be used to verify the integrity of the other seven bits. Parity may be set either to ODD or EVEN. Even (odd) parity means that the number of 1s in a byte is guaranteed to be even (odd).

Generally, two parity switches are provided:

- PARITY/NO PARITY and
- ODD/EVEN.

A program either uses parity, or it does not. If it uses parity, it may use either odd or even parity. Generally, all programs on a given computer follow the same convention.

When a program does not use parity, there is sometimes one more switch:

FORCED 1/FORCED 0

that systematically sets the value of the eighth bit to 1 or to 0.

Uppercase. Prior to transmission, all characters are automatically converted into uppercase characters. This is a convenience feature for the operator.

Reverse Video. Characters are usually displayed in white against a black background. With reverse video, characters are displayed in black against a white background. This feature is generally used under program control by specialized text processing programs for data input or word processing. Specific fields can then be displayed on the screen in reverse video.

When reverse video is manually selected by the operator via the switch on the CRT, the appearance of the entire screen is reversed.

Half/Full Duplex. Specifies the communication method used in communicating with the computer. Full duplex is used when both the CRT and the device that it is connected to are capable of both sending and receiving signals simultaneously. Half duplex is selected when transmission is possible in only one direction at a time. Any given computer always uses the same convention, generally full duplex. Some small home computers require half-duplex. Modems used for telephone communication require full duplex.

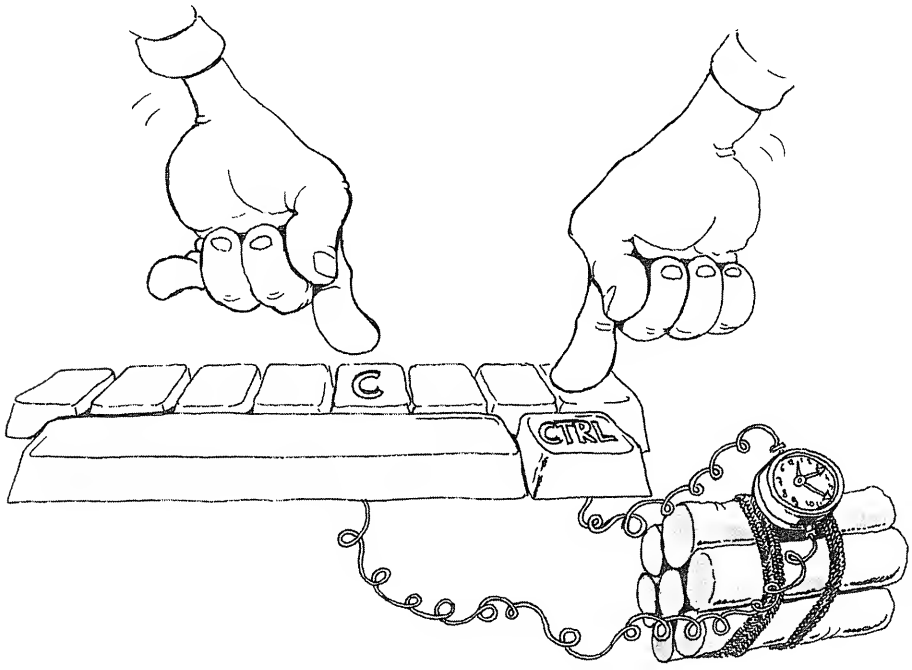
EIA/CUR Loop. Used to select the communication method for the modem interface on the back of the unit. EIA refers to the standard RS-232 interface, and CUR to the standard current loop interface. The communications method used with a CRT is generally determined by the type of interface on the computer.

The CRT is now correctly positioned and set. Let us use it properly.

Dangerous Keys

The effect of the keys on your keyboard is determined by the program you use and varies with different programs. When using the CRT, one essential recommendation applies: don't hit keys that might cause great damage, such as wiping out a file. Typically, the most dangerous keys are the "control" keys. Control keys are generally special keys, but may also refer to the simultaneous striking of the CTRL (Control) key together with another key. Sometimes, hitting the wrong control key can result in catastrophic damage, such as wiping out a program or file. In such cases, the "control" key should be clearly labeled in order to avoid inadvertent use.

For example, when typing text into a file, many editor programs or word processing programs allow a liberal use of the control keys, permitting control characters themselves to be inserted into the text. However, control characters *inadvertently* inserted amidst text or data may later result in a damaged text file or a file that is impossible to use or print. If this happens, first alert the operator, and then place a red dot, a raised label, or some other warning on the control key. Since the control key is generally very close to the shift key, it is easy for an operator to inadvertently strike it, rather than the shift key. The same recommendation applies to other "dangerous" keys such as BREAK, DEL (delete), and CLEAR.



Programmable Keys

Most business-type CRTs are equipped with a numeric keypad, or numeric cluster, designed to facilitate the entry of numeric data. A numeric keypad is shown on the right of the keyboard in Figure 6.1.

Many CRTs also offer programmable function keys that can be used to automatically send a short sequence of characters or commands to the computer. Many common functions of the operating system can then be encoded in a single programmable key. For example, if the "PRINT" command is used frequently, the programmable key P1 can be assigned the value "PRINT." Then by pressing P1, the "PRINT" command will be sent to the computer. This is a convenient feature that saves time and effort. Use it whenever it is available.

Connecting A Printer

Most CRTs are equipped in the back with one or more standardized female RS-232 connectors. The RS-232 connector allows the direct connection of a printer or a modem cable equipped with a male RS-232 connector. When a printer is attached to the CRT's RS-232 connector, everything that

appears on the screen of the CRT is simultaneously printed on the printer. However, printers operate at speeds slower than CRT terminals. Typically, a printer will operate at 300 to 2,400 baud, versus 9,600 or 19,200 baud for a CRT terminal. Therefore, before connecting a printer in parallel to a CRT terminal, the baud rate of the CRT must usually be reduced. The system may have to be restarted or reinitialized to tell the computer that the CRT is now operating at a slower speed. Some intelligent CRTs have a "buffering" capability, which allows a printer connected to the CRT to operate at a different baud rate than the CRT. However, in this case, an extra set of switches on the CRT must usually be set to the baud rate of the printer.

When the printer is disconnected from the CRT, remember to reset the CRT to the proper maximum baud rate. This same rule applies when a modem is disconnected from the CRT.

Moving The CRT

A CRT is normally attached to the computer via a standard RS-232 connector. It can be easily disconnected and moved away from the computer. The connecting cable may be as long as 100 feet, as long as it does not pick up electromagnetic noise from powerful machines or transformers along the way.

You may also use EIA/RS-232 extension cables. However, each additional connector increases the possibility of picking up EMI noise. When purchasing an extension cable, specify the number of lines in the cable, as various displays use different numbers of lines.

When connecting a keyboard-equipped printer to the back of your CRT, you may have to reverse lines 2 and 3 (data send/receive) of your cable. To do this, it is best to use a short "pin-reversal" cable (that reverses lines 2 and 3) between the printer cable and the back of the CRT.

EXTERNAL VIDEO MONITOR OR TELEVISION

In some personal computer systems, a direct *video output* is provided that allows direct connection of the computer to a home television or a video monitor, thereby eliminating the need for a full CRT terminal. The keyboard is then generally integrated with the computer proper. The same recommendations that apply to the CRT keyboard naturally apply to the integrated keyboard. Additional recommendations apply in the case of a television set or a video monitor.

The cable connecting the video output of the computer to the television set or to the video monitor is very sensitive to electromagnetic interference

and should be positioned for maximum image clarity. Moving the cable around may result in a significant image improvement or degradation. The best position for the cable is usually found by trial and error. To reduce interference, try tying a knot around a small ferrite core with the video output cable and placing the core inside the computer enclosure.

Whenever the RF (Radio Frequency) modulator that interfaces the television cable to the computer is accessible to the user, it should be tuned for maximum image clarity. This can be done by turning the adjustable potentiometer (adjustable resistor) of the modulator with a small screwdriver.

CRT SUMMARY

The CRT is easy to use, and it requires few adjustments and precautions. It should simply be kept clean and installed in a convenient location. The position of the CRT with respect to the operator is critical to comfort and effectiveness. We have indicated precautions that will result in reliable operation. When treated properly, a CRT will give you years of trouble-free operation.

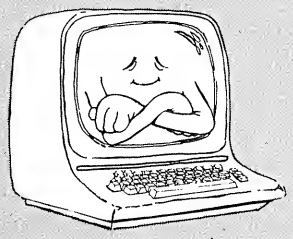
CHAPTER 7
THE PRINTER

Teeth placed before the tongue give good advice.
— Italian Proverb

FOR THE HOME COMPUTER USER

The essential recommendation, if you are using a printer, is:

Use all of the adjustments properly, and handle the printer gently.



INTRODUCTION

In most computer systems, the printer is the device that has the largest number of mechanical parts. It is therefore the device most likely to fail. However, if a high-quality printer is used only intermittently (say less than two hours per day), and operated properly, the probability of failure is normally small (say, once per year).

Because a printer has so many moving parts, it is particularly susceptible to rough or improper handling.

In this chapter, we will explain how to position the printer correctly and how to set the controls. We will also describe several important environmental requirements. We will then examine the four categories of printer failures and discuss specific remedies. Finally we will consider printer supplies.

TYPES OF PRINTERS

Many types of printers are manufactured, and new techniques are constantly being introduced. In a nutshell, the main types used with small computers are: dot matrix printers, thermal and electrostatic printers, daisy-wheel printers, and chain or other impact printers.

Dot matrix printers use needles which strike the paper through a ribbon to print characters formed from a number of dots. They are generally characterized by low cost, moderate to high speed, and, for the time being, poor appearance of the text.

Thermal and *electrostatic* printers burn characters into a special paper using a character matrix of dots or segments. They are generally characterized by very low cost, slow to moderate speed, and the inability to make multiple copies.

Daisy-wheel printers use a daisy-shaped printing wheel whose petals strike the paper. They are characterized by moderate cost, moderate speed and very high printing quality. They are used in most word processing applications.

Chain printers, and other types of impact printers, strike the paper in one or more positions at once. They are characterized by high speed, high cost, and acceptable printing quality. They are used for long printouts, such as reports, mailing lists and internal documents.

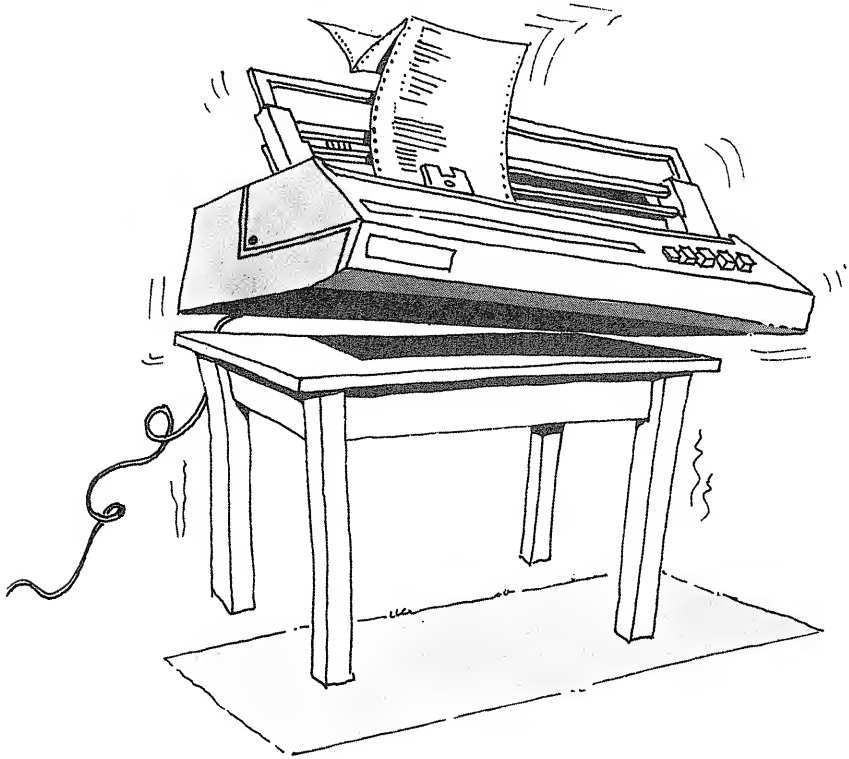
The recommendations presented in this chapter apply to all printers, with emphasis on daisy-wheel printers.

INSTALLING THE PRINTER

The printer should be positioned for stable operation, for unobstructed paper flow, and for easy operator access. Let us consider these three points in turn.

Printer Stability

The printer should be installed on a stable pedestal or support in order to avoid vibrations that will disrupt its operation. With most printers, ordinary light-weight tables are inadequate as they will move laterally and vibrate, which can create mechanical problems for the printer. Sturdy desks may be used, but specialized pedestals are best.



Paper Path Clearance

A typical paper path on a printer is shown in Figure 7.1. The box holding the paper used by the printer is normally placed in front of or under the printer. The paper is fed vertically through the printer as shown in (1) in

Figure 7.1. Then the paper must be correctly positioned on the paper advance mechanism. On a simple printer, this mechanism may simply be a pressure roller similar to the one on a typewriter. On printers used for business, a forms tractor is always used to properly position the paper. The paper must be properly inserted on this forms tractor with the holes matching the corresponding sprockets. This is shown in (2) on Figure 7.1. Once the paper has gone through the printer, it accumulates behind the printer in a basket attachment or in a box. This is shown in (3) in Figure 7.1.

The paper path imposes two requirements. There must be:

1. proper access to the fresh paper box and the printed paper box, for both the printer and the operator
2. proper positioning of the paper on the forms tractor.

We will now examine these two requirements.

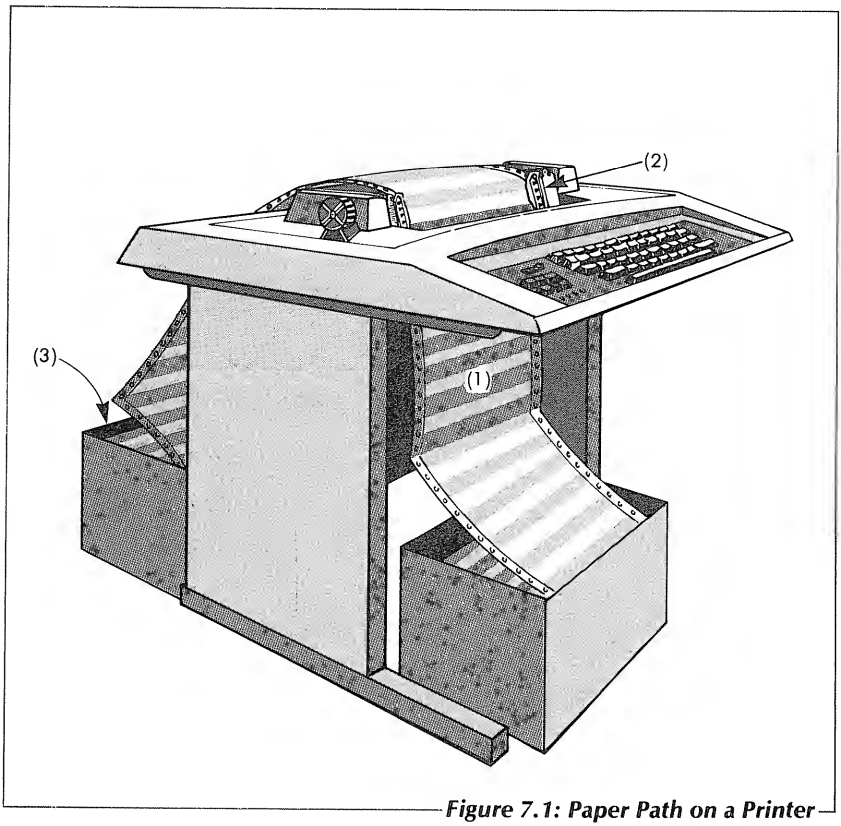


Figure 7.1: Paper Path on a Printer

Access To The Paper

Adequate clearance must be left on three sides of the printer. Space is necessary in front of or below the printer for the fresh paper box, behind the printer for the printed paper, and on one side of the printer for easy access to the printed paper box or basket behind the printer.

Positioning The Paper

The paper should be correctly inserted in the forms tractor on the printer. This point may seem rather obvious; however, it is easy to place the paper askew or to be inattentive or lax in setting the proper pressure

and position controls. As a result, a paper jam may occur inside the printer which could burn out one or more electronic boards.

We will now examine all the usual controls on a business printer, their roles and their proper uses.

Setting The Controls

First, put the paper in correctly. There is only one correct way to feed paper through the printer and the forms tractor. Learn it and respect it.

Then set the controls. Each printer has different controls and switches. However, most business printers provide the following main controls: pressure, roller disengagement, paper width, top-of-form and eject.

Pressure

It is almost always possible to adjust the amount of pressure exerted by the printing element as it strikes the paper. This adjustment will result in either a lighter or heavier printing. Proper adjustment is essential whether or not multiple copy paper or forms are used.

There are generally two ways to adjust the printing pressure. The head pressure adjustment is generally located on the head itself, or very close to it. It may not be very noticeable and the printer's manual should be checked for its proper use and identification.

In addition, a separate pressure control is generally available to position the pressure roller (see Figure 7.2.). This adjustment is analogous to the function of the lever in the upper left hand corner of an IBM Selectric

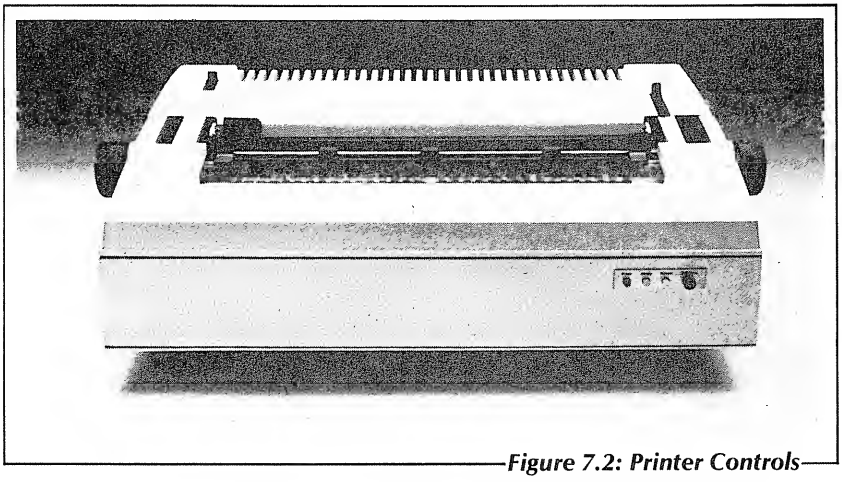


Figure 7.2: Printer Controls

typewriter and is intended for the use of thick paper or forms, so that printed characters have an unbroken appearance.

Two types of paper feeding are generally provided: friction feeding using a roller, and tractor feeding using a forms tractor. Friction feeding is only used for single forms or short printouts, as the paper will inevitably become misaligned. Tractor feeding is always used for continuous forms or paper.

Roller Disengagement

In the event that a sprocket feed is used, as in the case of a forms tractor, the pressure exerted by any roller mechanism must be relieved. Typically, business printers that have a pressure roller (like those on a regular typewriter), come equipped with a separate forms tractor attachment. When the forms tractor assembly is in operating position, the roller must be positioned so that the pressure exerted by the roller is released (see Figure 7.2). If this is not done, the printer will generally not operate correctly, and a paper jam is likely to occur.

Paper Width

The sprocket mechanism of the forms tractor is generally adjustable in width. Setting the width properly is required for correct system operation.

Additional Controls

There are two other switches that are also commonly available. They are TOP-OF-FORM and EJECT or FORM FEED. Whenever precise positioning of data is required on a form, the TOP-OF-FORM button must be pressed. This "tells" the mechanism that the next line to be printed is the first line on a page or form. The EJECT or FORM FEED switch can then be used to move the printing mechanism and/or paper to the top of the next page, i.e., to the first printing position on top of the next page.

Printer Controls Summary

Additional controls may be available on various printers, but they are generally less important. It is essential that the operator understand the function of the pressure controls. For example, if the printing mechanism is positioned too far from the paper, the printout may be readable although somewhat weak. However, the printer may fail at random intervals. The reason for this is quite simple: when the distance from the printing head to the paper is too great, the time needed by the head to travel to and

from the paper may be too long for some sequences of characters. The result is that either some characters are missed, or the printer or the driving software lock up. This problem may be hard to diagnose. Before using the printer, always check to insure that all controls are set properly. Don't neglect any lever, including the "paper thickness" lever.

CONNECTING THE PRINTER

A printer is attached to the computer either via a serial or parallel interface. Make certain that the cable connectors are properly attached and secured at both ends, and that inadvertent pulling of the cable will not dislodge or bend any of the pins on the connectors at either end.

Recall that a serial printer may also be connected to the back of most CRT terminals. CRT terminals are generally equipped with one or more standard RS-232, 25-pin connectors on the back. The printer may then be connected "in parallel" to the screen by plugging the printer cable into the connector on the back of the CRT unit. The speed of operation of the CRT must then be reduced to the speed of the printer by setting the proper switches on the CRT terminal and by telling the control program on the computer that the CRT speed has been modified. This may require restarting the computer system. Sometimes the CRT speed may be adjusted from the CRT terminal itself, depending on the software used.

Some printers are equipped with a keyboard and can be used as a terminal (see Figure 7.3). A printer that is used as a terminal requires a different cable attachment than a receive-only printer. It also requires a special software driver in order to communicate with the computer.

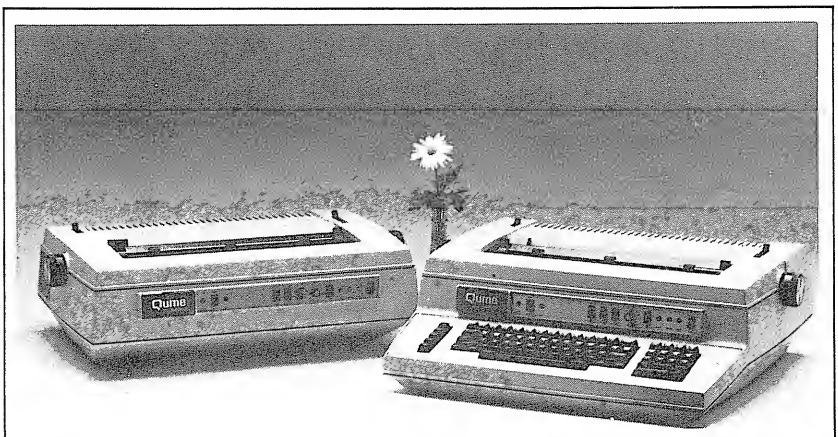


Figure 7.3: Daisy-Wheel Printers, With and Without Keyboard

One more note of caution: when using programs that specialize in formatting text, such as text and report formatters or word processors, these programs must be specifically adapted to the printer that you are using. Each printer has different positioning and printing controls, so that specific software drivers are necessary in order to take advantage of these facilities. In particular, if a word processor is not tailored for the printer to which it is attached, all of the features of the software and the printer may not be usable.

When changing either software or hardware on your system, remember that the software and hardware within a system must be compatible. Changing a peripheral in a computer system, such as a printer, often requires a change (a patch) in the operating system, as well as in specialized programs, such as word processing programs, that operate the terminal directly.

THE ENVIRONMENT

Since modern printers incorporate one or more boards of integrated circuits, power and environmental requirements are similar to those of the computer itself. A typical operating temperature is 35° to 110°F (1.0° to 44°C) with 40% to 95% relative humidity.

Whenever the relative humidity is low, problems may occur with static build-up on the paper. It may be necessary to use static-discharge brushes with high-speed printers operating in a dry environment. These brushes should be positioned on the back of the forms tractor, so that the paper will fall correctly behind the printer.

Printer paper is best stored at 75°F (24°C) at 45% relative humidity. The recommended range is 64°F to 75°F (18°C to 24°C) at 40% to 60% relative humidity.

As usual, liquids should be kept away from the printer mechanism. Here is another horror story.

Holding a cup of coffee, an anxious manager is waiting for a report to be printed. He enters the computer room, to examine the output of the printer while it is being printed. He does not have good eyesight, and he leans forward in order to more closely examine the material

being printed. Liquid spills onto the printer mechanism and the control electronics, causing tragic damage.

Managers and other intruders should be expressly warned against carrying liquids in close proximity to the computer system.

MAINTENANCE

Printers usually require little maintenance. Preventive maintenance is highly recommended and its frequency varies with the type of printer and its usage. For example, for a typical daisy wheel printer, the recommended time interval is usually six months or 500 hours of use. During a maintenance visit, the three main operations are cleaning, verification of the mechanical adjustments, and, at times, lubrication. Such preventive maintenance should be performed by qualified personnel.

The user is responsible for keeping the printer clean. In particular, the user should make sure that all ventilation openings are kept clear of dust and debris. Recall that paper debris tends to accumulate in the printer area, which may clog ventilation openings or delicate parts of the mechanism. Periodically, the user should disassemble the top of the printer and look for dust and debris. When found, dust should be wiped off with a lint-free cloth, vacuumed, or simply blown away.

In order to minimize the stress on a paper feeding mechanism, at the end of a printing, always tear the paper along the perforations. Don't tear the paper sideways or you may eventually bring the mechanism out of adjustment. Always advance the paper beyond the sprocket wheels and hold the bottom part of the paper while you are tearing the top part.

Finally, as in the case of electronic or mechanical equipment, no paper clips, staples or pencils should be left on top of the printer. If any object should fall inside the printer, be sure to turn off the printer and remove the power cord from the wall socket before attempting to remove the object from the mechanism.

Dismantling the Printer

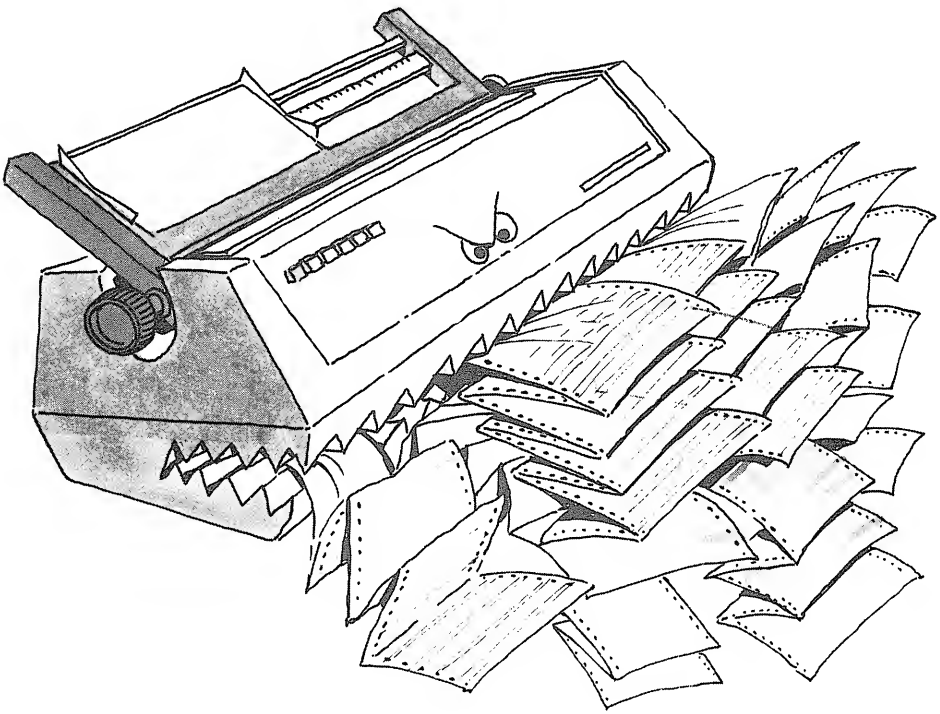
Removing the top elements of the printer (roller and other components) is part of standard operator maintenance. Similarly, when a paper jam occurs or when paper debris accumulates inside the printer, it is necessary to remove the forms tractor, the roller and other parts of the mechanism that are removable. Typically, this involves removing several parts. It is important that an operator know how to assemble and disassemble the top of the printer in order to be able to remove debris.

PRINTER FAILURES

So, despite proper adjustment and care (or perhaps for the lack of it), your printer has failed. Let us examine the main causes and remedies. There are four types of problems that can occur:

1. paper jams
2. erratic behavior
3. electronic failures
4. mechanical problems, such as an end-of-ribbon or a broken printing element.

Let us now examine each of these problems in turn.



Paper Jam

A paper jam is due to a physical obstruction. The jam is usually caused by incorrectly set controls, by improper paper placement, or by using forms not suited to the printer.

When a jam occurs because controls are set incorrectly, the problem is likely to occur soon after the printer is started. Therefore, any time that a printing operation is started, it is essential that the operator observe the printer for several minutes before leaving the room, to verify that it is operating properly.

A paper jam may be caused by an accumulation of paper behind the printer or by a problem with the paper path in front of the printer. In such a case, the jam may occur only towards the end of the printing.

When a paper jam occurs, the printer may burn out. Burnout may involve the printing mechanism, or printed circuit boards, or both. It is therefore recommended that an operator watch (or listen to) the printer continuously. Whenever a printing operation is likely to go on for a long time, it is very tempting for an operator to leave the room and thus leave the printer

unattended. If this happens, someone should at least monitor the noise made by the printer. If the noise stops suddenly or changes pitch, either the printing operation is finished, the paper or ribbon has run out, or a paper jam has occurred.

Leaving the printer unattended may allow some printers to continue printing merrily along while the fresh paper has run out. Many printers will automatically stop when they run out of paper; however, some printers will simply go on printing. If this occurs, the printing element will usually be damaged. However, running out of paper is not as dangerous to the printer as a paper jam. Special self-stick items such as self-adhesive labels or envelopes are likely to cause paper jams. When using new forms for the first time, which involve detachable items, be sure to continually watch the printer. A single label may become attached inside the printing mechanism, and cause a malfunction or a paper jam.

Make a note of the proper lever settings for various kinds of paper. Often, an alternative type of label or stationery is substituted to solve a printing problem, when, in fact, a mere change in the control settings would have been sufficient.

Erratic Behavior

Sometimes, the printer will start skipping or misprinting one or more characters or lines. This may be caused by four main problems:

1. operator mis-setting
2. mechanical printer problem
3. software problem
4. hardware problem

In some cases, erratic behavior is caused by improper settings on the part of the operator. Therefore, the first thing to do is to check for correct settings. If the settings are correct, then improper mechanical adjustments should be suspected.

Most often, erratic behavior is due to a faulty mechanical adjustment inside the printer. Maintenance specialists should be called in to correct such adjustments.

However, there is always the possibility that software, i.e., the program, may be causing the erratic behavior. If the software was operating properly in the past, i.e., it was proven correct, it is usually a simple matter of substituting a backup copy of the program. If the problem disappears when this

is done, then the software support was simply damaged and the cassette or diskette containing the suspect programs should be replaced. If substituting the backup copy of the software doesn't solve the problem, then hardware must be suspected.

Another possible cause of erratic behavior may be an improper linkage between the computer and the printer. It is important to carefully check the cables, including the attachment of the cables to the computer and the printer. All contacts should be clean, properly attached, and stable. As a last resort only, visually inspect the interface board to which the printer is connected. In most cases where the board is at fault, one or more pins or wires have come loose due to improper cable placement or frequent disconnections.

A general principle of diagnosing problems, is to use the substitution technique whenever possible. First try to determine whether the problem lies *within* the printer or *outside* of it. The simplest method is to bring in another printer of the same model and to substitute it for your printer. If the new printer works well, using the same settings, then your printer is at fault. However, if the new printer also malfunctions, you may still be using the wrong settings, or else the problem lies outside the printer.

If the problem seems to be outside of the printer, replace the interconnection cable with another one, if available. Test the printer again, and if it still malfunctions, replace your software diskette with another one (the backup copy). Finally, replace the printer interface board with another one, if available. If any of these substitutions solves the problem, you have identified the culprit. (This strategy was proposed by Caesar in Roman times as "divide and conquer.")

Electronic Failure

An electronic failure within the printer's circuitry, or within the computer system itself, will result in failure of the printer. Most printers are equipped with an ERROR/ALARM light that will indicate to the user that some malfunction has occurred, even though the printer may continue operating past this point.

An electronic failure within the printer usually results in gross misbehavior. Repair should be left to a maintenance specialist. However, if an electronic failure is suspected, it can often be cured by merely pulling out the internal printer boards (with the power off, of course), and cleaning the contacts and pushing all integrated circuits firmly into their sockets to insure proper contact. If this technique fails, a maintenance technician must be called. The usual technique used by the maintenance technician

also relies on the "divide and conquer" strategy: The technician swaps a replacement board in each of the slots in turn until the faulty one has been identified.

Mechanical Failure

The three most common types of mechanical failure on the printer are:

1. failure of the printing element, such as a printing wheel
2. failure of the ribbon
3. failure of the advance mechanism.

In the first two cases, the symptom is that one or more characters do not print anymore or that they print weakly. In such a case, the printing element or the ribbon should be changed. If the printer is a dot matrix printer and some of the dots print very weakly, the pressure of the head should be adjusted, but if the problem is more significant, a maintenance specialist should be called.

There are two types of ribbons: cloth and carbon. The cloth ribbon is normally used on a printer. It may be used several times; however, the contrast diminishes each time it is used. The cloth ribbon normally reverses direction automatically when it reaches the end of the roll.

Cloth ribbons have two advantages: First, they are inexpensive. Second, the contrast of the characters fades out slowly, so that if the contrast is high at the beginning of a long document it is likely to be acceptable by the end of it.

The carbon ribbon is more expensive than the cloth ribbon and is used only in situations that require the best printing quality, such as the preparation of a camera-ready document. Most carbon ("film") ribbons are usable *only once* and stop abruptly when the end of the ribbon has been reached. Most printers will keep printing even though the carbon ribbon has stopped. As a result, if the printer is left unattended, the beginning of the document may be correctly printed, while the rest of it will be left blank. When using a carbon ribbon, note the length of the ribbon remaining in the cartridge before you begin a long printing.

Also, learn how to properly insert both types of ribbons. If ribbons are inserted improperly, they are likely to get stuck and will give the appearance of a malfunctioning printer. If this happens, simply take the ribbon out and insert it again properly.

Finally, a common mechanical malfunction is uneven spacing between lines. This problem involves the paper advance mechanism and requires an adjustment by a specialized technician.

Failure Summary

Let us summarize here the main recommendations in the case of a total or partial printer failure.

Step 1: First check the mechanical adjustments:

- Check the power and connection cables to the computer for proper positioning and insertion.
- Check all operating switches and controls for proper settings.
- Check the fuses.
- Check the printing head or mechanism, the ribbon, and the paper.

Step 2: If nothing works, turn everything off, including the computer system, and restart the system.

Step 3: Use a fresh copy of the software, and execute Step 2 again.

Step 4: If the printer *almost* works, check all settings again, verify the paper path, the head striking force, the ribbon. Verify the proper electrical environment: clean power, no static. If this fails, try substituting the suspected elements: printer, cables, and boards.

Step 5: If all fails, give up, and call the maintenance personnel.

When a powerful high-speed printer is being used, the power surge caused by turning the printer on or off may disrupt the operation of the computer or disk drive. In such a case, either the printer should be connected to a separate electrical line, or a line isolator should be used.

SUPPLIES

We will now present practical recommendations regarding the use of appropriate printer supplies and their proper storage.

In addition to spare fuses, the printer requires three types of supplies: paper or business forms, ribbons and, in the case of daisy-wheel printers, print-wheels. Many types of paper and forms may be used. Let us examine the main categories.

Paper

Several types of paper and forms may be used with a printer. Let us examine them in turn.

Computer Paper

Computer paper for use on a forms tractor comes with two columns of holes that run down each side. Also called *fan-fold paper,* this paper consists of a continuous length of sheets joined with perforations and folded

in a zig-zag fashion. It can be continuously fed and folded without operator assistance. The paper comes in many qualities and widths. If you know the maximum width that you will need, you should use the narrowest paper that will meet that need, in order to minimize cost. For example, if you type many business letters or drafts in an 8-1/2'' × 11'' format, you can buy perforated paper which will yield 8-1/2'' × 11'' pages with little waste. If you require the full width of your printer (120 or 132 columns), then wider, regular-sized computer paper is necessary.

Computer paper is also available in a multi-layer format with carbons pre-inserted or with automatic carbons. Such paper is more expensive, but will minimize the printing time required to produce multiple copies.

Ordinary paper may be run through the printer twice for working documents. Printing on both sides of the paper in succession results in obvious savings.

Preprinted Forms

Preprinted stationery or forms are used for computerized letters, for invoices, statements and other form preparation. Three types may be used:

1. forms printed on continuous paper
2. forms glued on continuous paper
3. regular, single-sheet business forms.

Business forms may be printed directly on continuous computer type paper; a number of suppliers will customize and print them for you. Alternatively, regular letterhead paper and envelopes can be attached to continuous computer paper. After going through the printer, they are separated by hand (or machine) from their continuous support. Finally, special attachments can be used in order to automatically feed regular letterhead or forms into the printer (see Figure 7.4). In all cases, the result is computerized letters or forms that look as though they have been individually typed on a typewriter.

Labels

When printing mailing lists on adhesive labels, you should know that labels come in a variety of shapes and sizes. They may be single column labels, 4 column labels, or some other format. The number of lines per label can also be specified. Generally, using labels mounted in four columns on continuous backing results in higher printing speed, since the printing element is not required to come back to the beginning of the line as frequently. This is called a 4-up format.

Ribbons And Wheels

Spare ribbons and printing elements should always be available in the computer room, since they may be needed for replacement at any time. Cloth ribbons should normally be used unless the high quality of carbon ribbons is required. The two main disadvantages of carbon ribbons are: high cost and the possibility of a sudden stop. When daisy-wheel printers or other printers with removable printing elements are used, spare wheels or printing elements should always be available. Wheels are best stored in special boxes, as shown in Figure 7.5.

Other Supplies and Equipment

Spare fuses are another item that should always be kept on hand. Specialized storage racks and caddies are available to facilitate the storage and retrieval of computer printouts, as shown in Figure 7.6. Finally, any

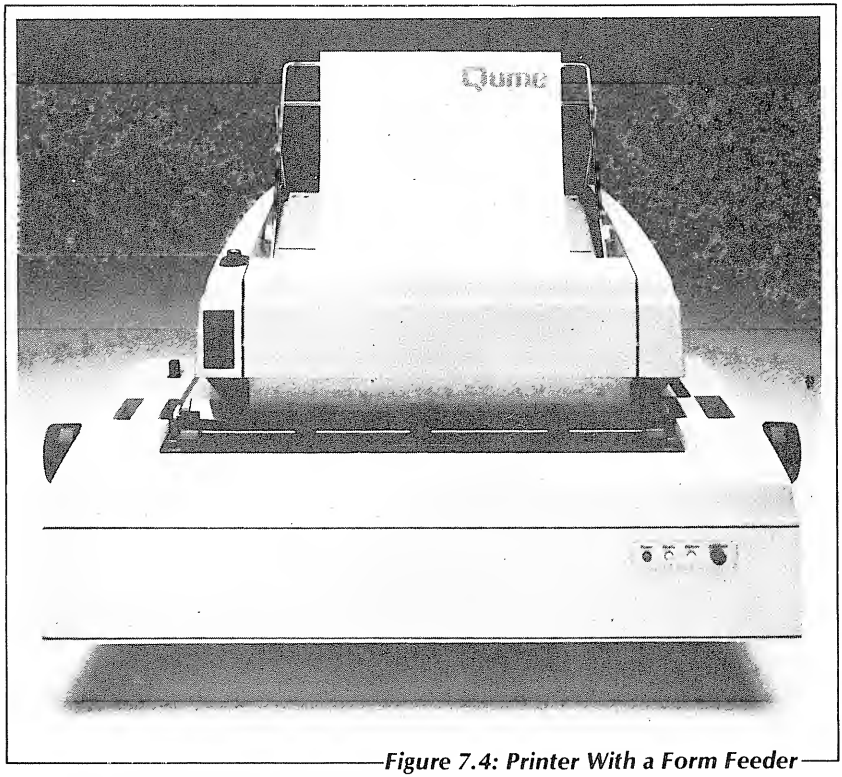


Figure 7.4: Printer With a Form Feeder

time that a printer is used for business purposes, you should consider the use of a shredder. This topic will be addressed in Chapter 12.

PRINTER SUMMARY

The printer is usually the most complex mechanical device in a computer system and requires manual adjustments not required with other devices. It should be properly installed and positioned, and the user must know the purpose of the various levers and adjustments and how to set them.

In order to reduce the possibility of a burn-out, a printer should always be monitored by sight and/or sound.

Failures are generally due to mechanical causes and can therefore be reduced by proper operator training. Most printers will operate reliably provided the settings are used properly and preventive maintenance is performed regularly.

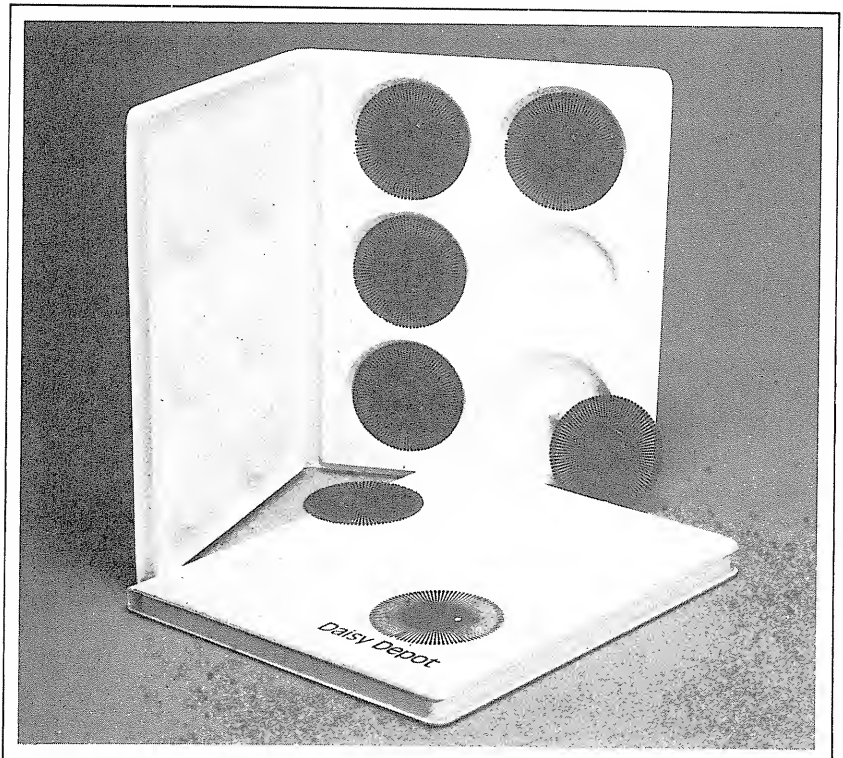


Figure 7.5: A Daisy-Wheel Storage Box

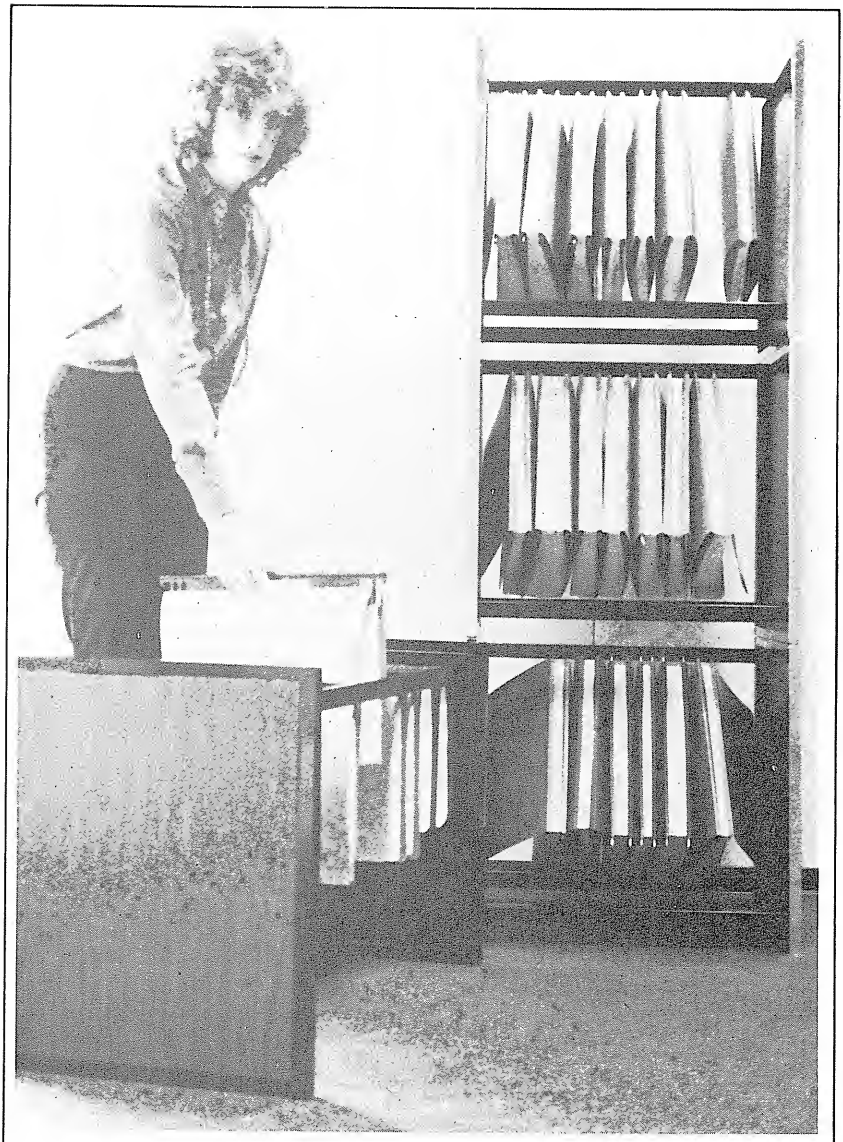


Figure 7.6: Printout Caddy and Rack

CHAPTER 8
THE TAPE UNITS

Learning without thought is labor lost; thought without learning is perilous.
— *Confucius,* Analects, Bk. 2:15

FOR THE HOME COMPUTER USER

Tape units used in a home environment are always cassette units. When using a cassette unit, five essential recommendations apply.

Keep the cassettes dust-free and periodically clean the recording head.

Use cassettes of the proper format and quality. Cassettes used to store data differ from regular cassettes in three ways:

- There is no leader on the tape, so that the tape is usable at both ends.
- The magnetic coating on the tape is generally of a higher and more uniform quality.
- The mechanism of the cassette itself is of a higher quality than a standard dictation cassette.

Use the write-protect notch. Cassettes are equipped with a write/protect notch on the back of the cassette. When this notch is pushed in, it is no longer possible to write information on the tape. This protects the contents of the tape from accidental overwriting.

Use a double recording technique. Frequently, the cassette recorder is of low quality. In such a case, use a double recording technique, i.e., record each program or set of data (a *file*) twice on the same tape. Then, if it becomes impossible to read the first recoding of a file from the cassette, there is a good chance that it will be possible to read the second recording correctly.

Make a note of the proper volume adjustment. Most home computers are quite sensitive to the output level used on the cassette player. Make a note of the proper level on each cassette you use.

INTRODUCTION

The principle of operation of all tape units is the same: information is stored on the magnetic surface of the tape as a sequence of bits (0s and 1s). Tapes can be used to store a large quantity of information economically (millions of bytes, i.e., characters). However, access to the information on a tape is sequential, and winding or rewinding a tape is slow compared to accessing information on a disk. Tapes are therefore normally used only for storing large amounts of data economically, or for transferring information from one computer to another.

Two main types of tape drives are used with computers: the cassette recorder and the "industry-standard" (IBM type) tape drive. The *cassette recorder* is normally used with the inexpensive, home-type systems; however, it is also sometimes used on business terminals for ease in exchanging or transferring programs between users. The main advantage of the tape cassette is that it is inexpensive. Its two disadvantages are that it is slow and it stores a limited amount of information.

Conversely, the *industry-standard tape drive* is expensive and is used for its high storage capacity. In most newer installations, a tape drive is used primarily to back-up a hard disk unit. Because of its sequential access and high cost, the tape drive is generally not used in small business installations. Instead, a removable disk pack or disk cartridge is generally preferred.

High-speed *cartridge tape units* are also used to back-up disks, in particular Winchester disks. A typical cartridge uses 1/4 inch, 450 foot tape and holds 20 megabytes of unformatted data. It operates in the streaming mode, recording data at 30,000 bytes per second and 8,000 bits per inch, thus making it possible to backup a 20 megabyte disk in 12 minutes.

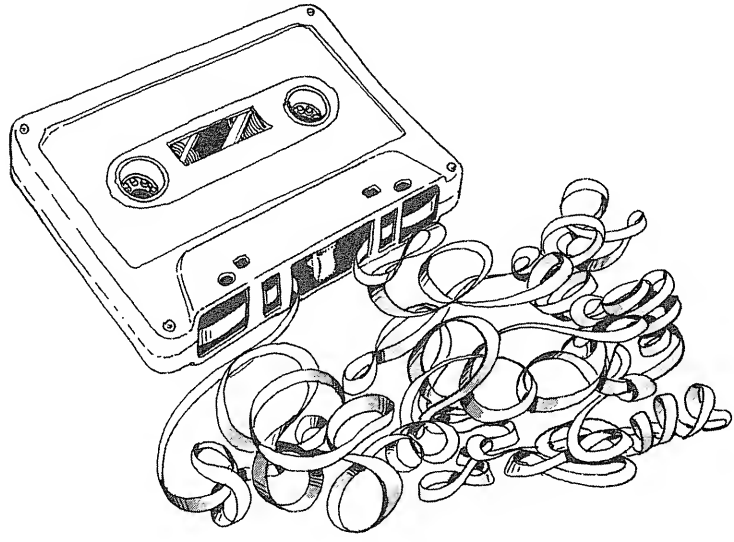
The recommendations presented in this chapter apply essentially to standard tape drives.

Magnetic tapes are less sensitive to shocks, dust and magnetism than hard disks but should still be treated delicately. In this chapter, we will examine the proper handling of a tape, the required environment, and proper tape storage and shipping. We will then consider specific tape problems, and maintenance procedures. The most important precautions apply to proper handling. Let us examine them.

HANDLING A TAPE

The recommendations for handling a tape are simple and straightforward. Most are DON'Ts:

- Don't touch the surface of a tape. The oil from your skin will damage the magnetic surface. Fingerprints, whether on the magnetic oxide or on its backing, will also hold dust and lint. Contamination will then spread to the drive and to other tapes. Use lint-free gloves whenever possible.
- Don't let the magnetic surface of the tape come in contact with dust or liquids. This includes the tape drive mechanism, which should be kept clean at all times. Watch for paper dust generated by line printers.
- Don't smoke near a tape drive.
- Don't bring magnets or magnetic coils near tapes.
- Don't squeeze reel flanges, or you may cause tape edge damage during winding/rewinding. Handle tapes with care. Handle reels by the hub hole. When mounting the tape on the drive, apply pressure on the hub, not on the flanges.
- Don't use a damaged tape. Watch for possible warping and cracks on the tape.
- When using cassettes, make sure that the tape is tight on both reels. If the tape is loose on one side, insert a pencil through one of the cassette holes and turn it gently until the tape is tight. Don't stress the tape, as you might stretch it and lose data.



- Before using tapes that have been brought in from the outside, allow them to equalize temperature within the computer room. Allow 24 hours, as in the case of disks, for large differences in temperature, or physical distortion may result.
- Open tape cannisters in a clean atmosphere only.
- Close the tape cannister promptly.

In summary, handle tapes gently and prevent contamination.

ENVIRONMENT AND STORAGE

Tapes should be used and stored in a clean environment at a proper temperature. The recommended temperature range is 15° to 50°C (59° to 122°F).

As in the case of disk units, the room should be kept free of dust and lint. Avoid storing paper stock and cardboard in the room in order to avoid paper dust. In order to keep pollutants out, the air pressure within the room may be increased. If necessary, install the printer in a low pressure area, and the tape drives in a high pressure area. There should be no smoking, eating or drinking in the room. Smoke will not damage tapes, but ashes will. Debris or droplets of liquid from food items may be propagated from the hands and contaminate a tape.

Cassette tapes should always be stored in protective boxes or in specially designed cassette binders or holders. These containers will protect cassettes from dust and will also lock the cassette wheels in position, thus preventing the tape from loosening up (see Figure 8.1).

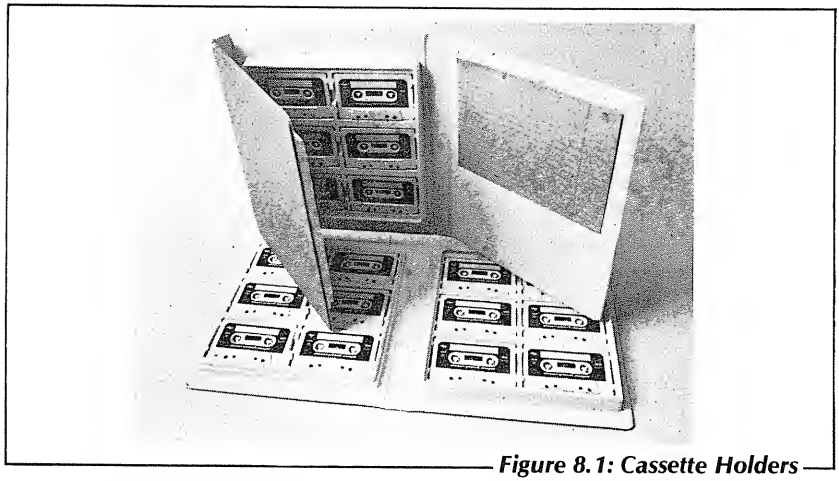


Figure 8.1: Cassette Holders

Tape reels should be stored in air-tight cannisters and shelved vertically rather than horizontally (see Figure 8.2). Horizontal storage may result in stress on tapes at the bottom of the stack or in the accidental fall of a magnetic tape.

When storing tapes, use a low wind tension (about 7 ounces (196 grams) per 1/2'' of tape width). If you use a higher wind tension, backing distortion may occur, especially if the temperature rises. However, don't use too low a wind tension, or *slippage* or *cinching* will occur. The effect of slippage is shown in Figure 8.3. Cinching shows as wrinkles on the tape and is shown in Figure 8.4. If cinching occurs, rewind your tape again promptly, using the proper tension. Winding should be performed smoothly and uniformly. In particular, no tape strands should stick out on the sides.

Traditionally, tapes were rewound at periodic intervals to relieve internal pressures. This practice is no longer required with good quality tapes, but may be done as a precaution with lesser quality tapes.

When a tape is stored, inspect it for obvious problems such as loose winds, uneven edges, visible distortion, cinching, and dust. When many tapes are stored for extended durations, use *control tapes,* and check them periodically.

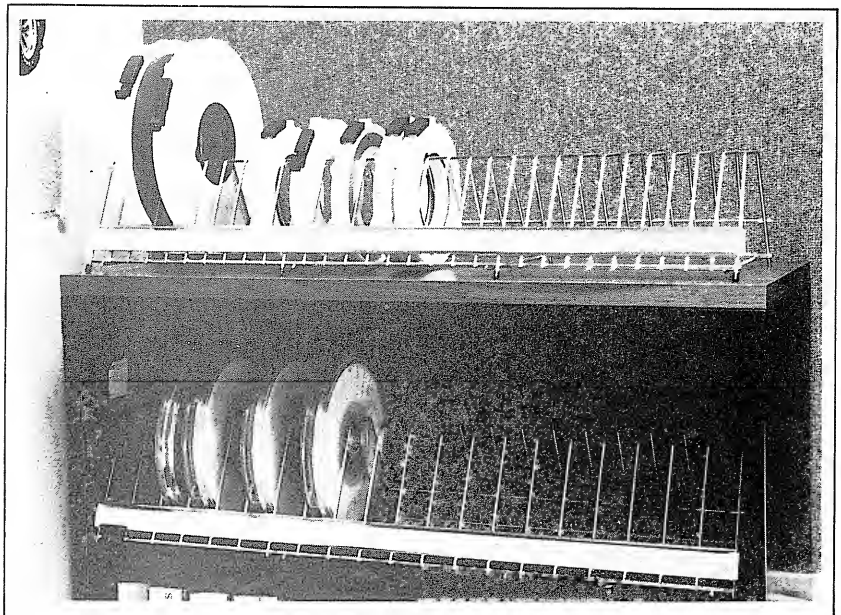


Figure 8.2: Vertical Storage Rack for Tape Reels

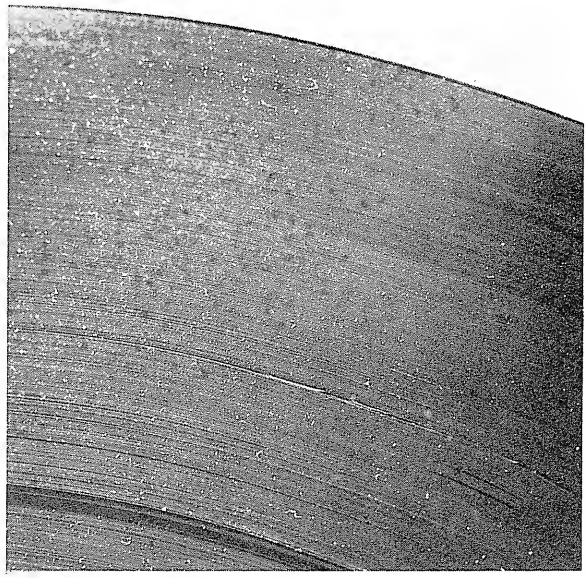


Figure 8.3: Effect of Tape Slippage

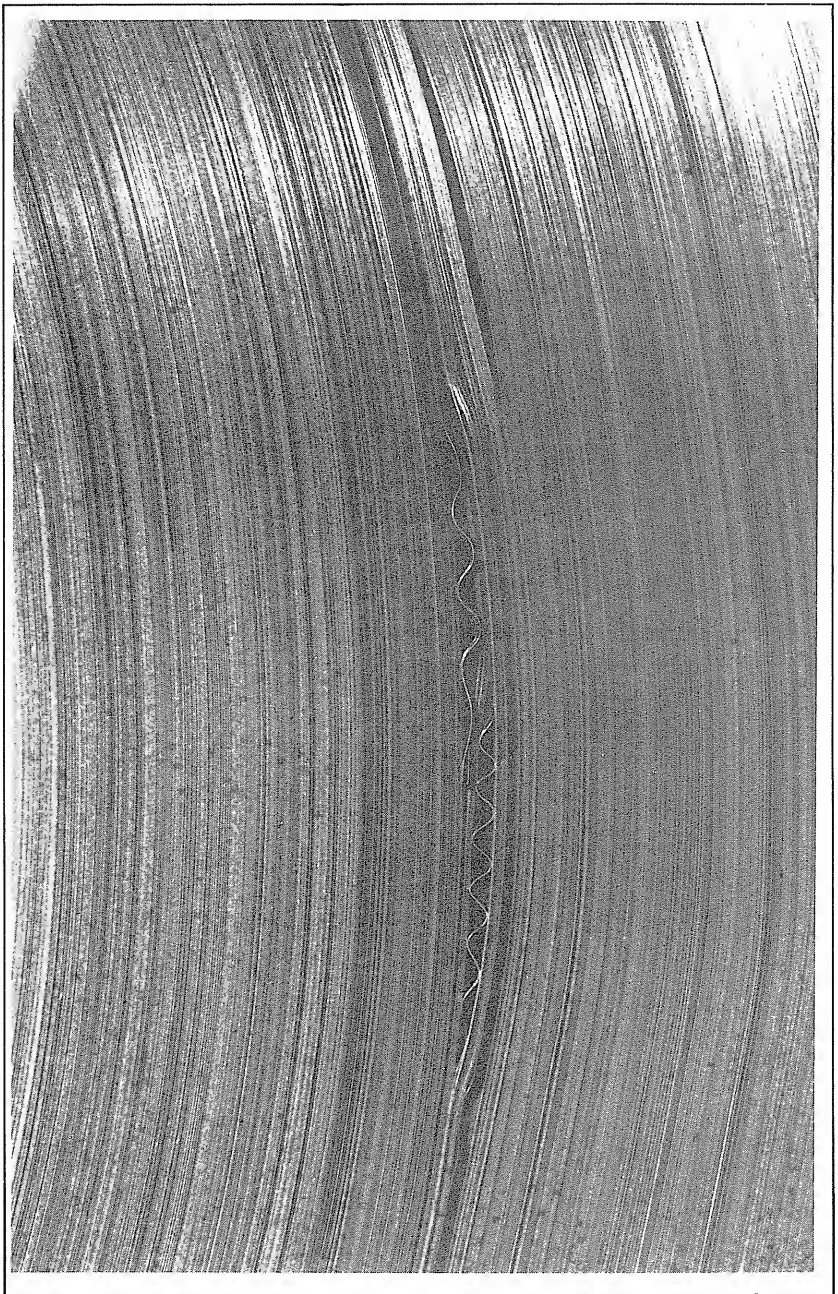


Figure 8.4: Tape Cinching

In case of fire, a temperature of 120°C (250°F) will cause permanent damage by distorting the backing. Use a CO_2 extinguisher to extinguish burning tape. Water should not be used as it causes a transverse curvature of the tape, called *cupping*. If tape reels are flooded, let them dry at normal temperature, rewind them twice, then hope for the best. Next time, store them in cannisters.

Finally, don't worry about radioactivity. Tapes are immune to nuclear radiation, including a neutron bomb, and radioactive fallout.

SHIPPING TAPES

Tapes should be protected from accidental unwinding, humidity, distortion, magnetic fields, and temperature extremes. Use a special container which is rigid and waterproof, as shown in Figure 8.5.

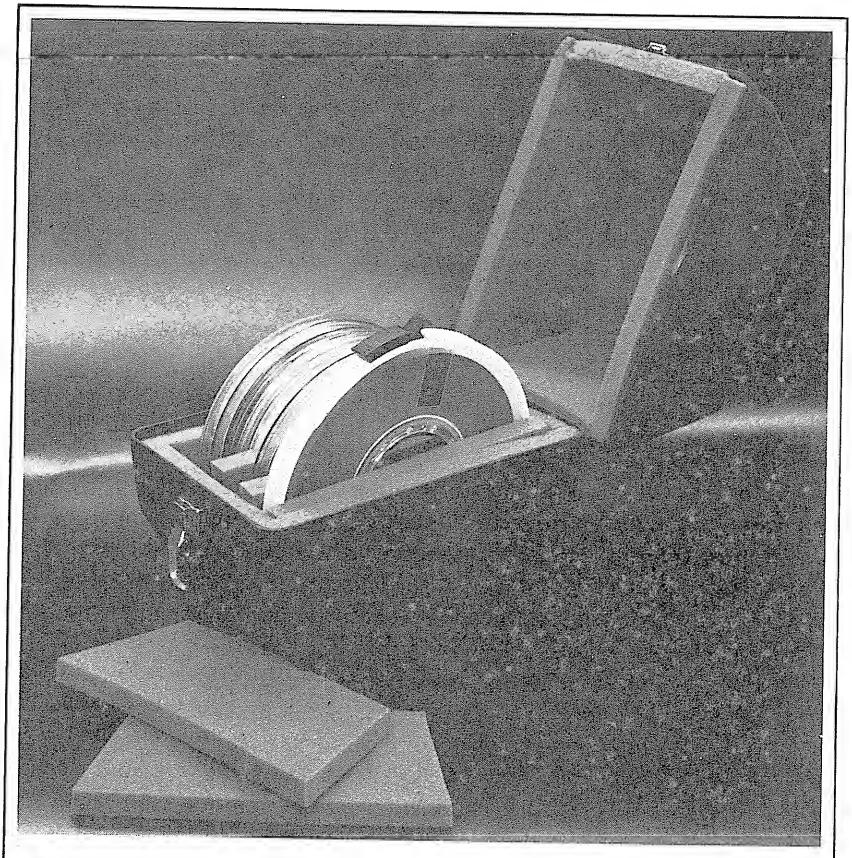


Figure 8.5: Tape Container

A foam lining and a rigid shell are used for shock protection. The free end of each tape must be well secured. For best results, use both a vinyl strip and a hold down sponge to secure the ends. If the tape is exposed to cold temperatures, the backing of the tape will contract, and the strip may come loose. In case of shock, the sponge may come loose, but normally the strip won't.

The magnetic protection of the tape is achieved by keeping it at a safe distance from a magnetic source. For total protection, allow 3'' of bulk spacing around the tapes.

TAPE PROBLEMS

Tape reading problems are often called dropins, dropouts, error growth, and print-through. They all refer to the fact that the information stored on the tape has been lost or altered.

Dropins refer to the presence of spurious bits on the tape, due to print-through or other magnetic influence. *Dropouts* refer to lost bits of information, because of tape damage, magnetic influence, or a defect. *Error growth* refers to the enlargement of a problem area, generally because of static or contamination.

Dropouts and error growth are often caused by polyester debris from scratches on the tape backing, or by the attraction of airborne debris through static. The remedies are proper cleaning, avoidance of air pollution, and proper humidity.

Print-through is caused by a tightly wound tape on which the recorded data remain in a static position for too long. Often, in such a case, combinations of bits on one layer eventually affect the next layer of magnetic coating, changing 0s to 1s, and vice versa. Data is then lost. Frequent rewinding solves this problem.

In addition, we have already mentioned *shifting:* rotational shifting causes cinching of the tape. Lateral shifting causes damaged tape edges. Both are prevented by winding the tape at the proper tension.

Tape stretching also results in incorrect readings, since it modifies the physical distance between successive bits on the tape. Again, proper winding prevents this problem.

Edge damage may have two adverse consequences: loss of the information contained in the edge track, and contamination across the entire width of the tape by edge debris. Edge damage may be caused by the operator, the drive, or the reel. In order to prevent edge damage, don't handle the tape by the flanges, and inspect transport guides and heads for any unusual buildup of particles. This buildup may be an accumulation of magnetic oxide or debris from the tape backing, and clearly indicates a

problem. Whenever errors are detected on the edge track only, you probably have a tape drive alignment problem.

Finally, as a preventive measure, use high-quality tapes. Low-cost tapes are often certified by having defects smoothed out. The result is illustrated in Figures 8.6 to 8.8. A non-uniformity on a tape being certified is first detected (Figure 8.6) and then repaired (Figure 8.7) by smoothing it out or scraping it. The tape can then be certified, but eventually, the problem reappears (Figure 8.8).

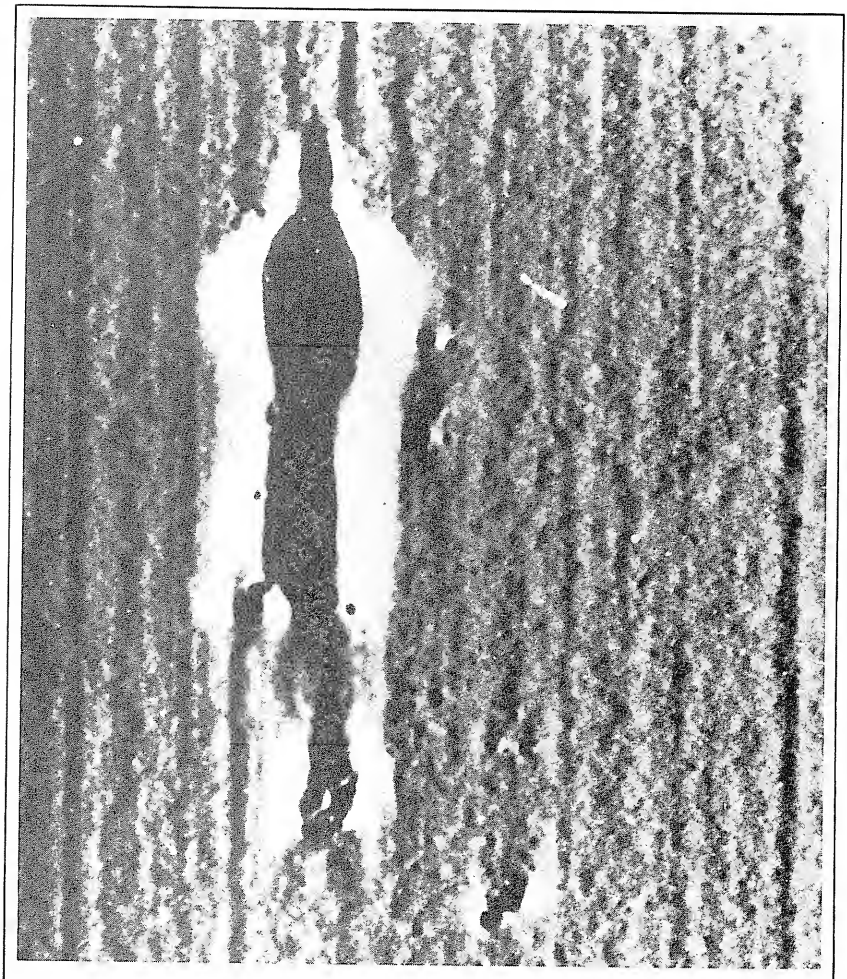


Figure 8.6: Tape Non-Uniformity upon Detection

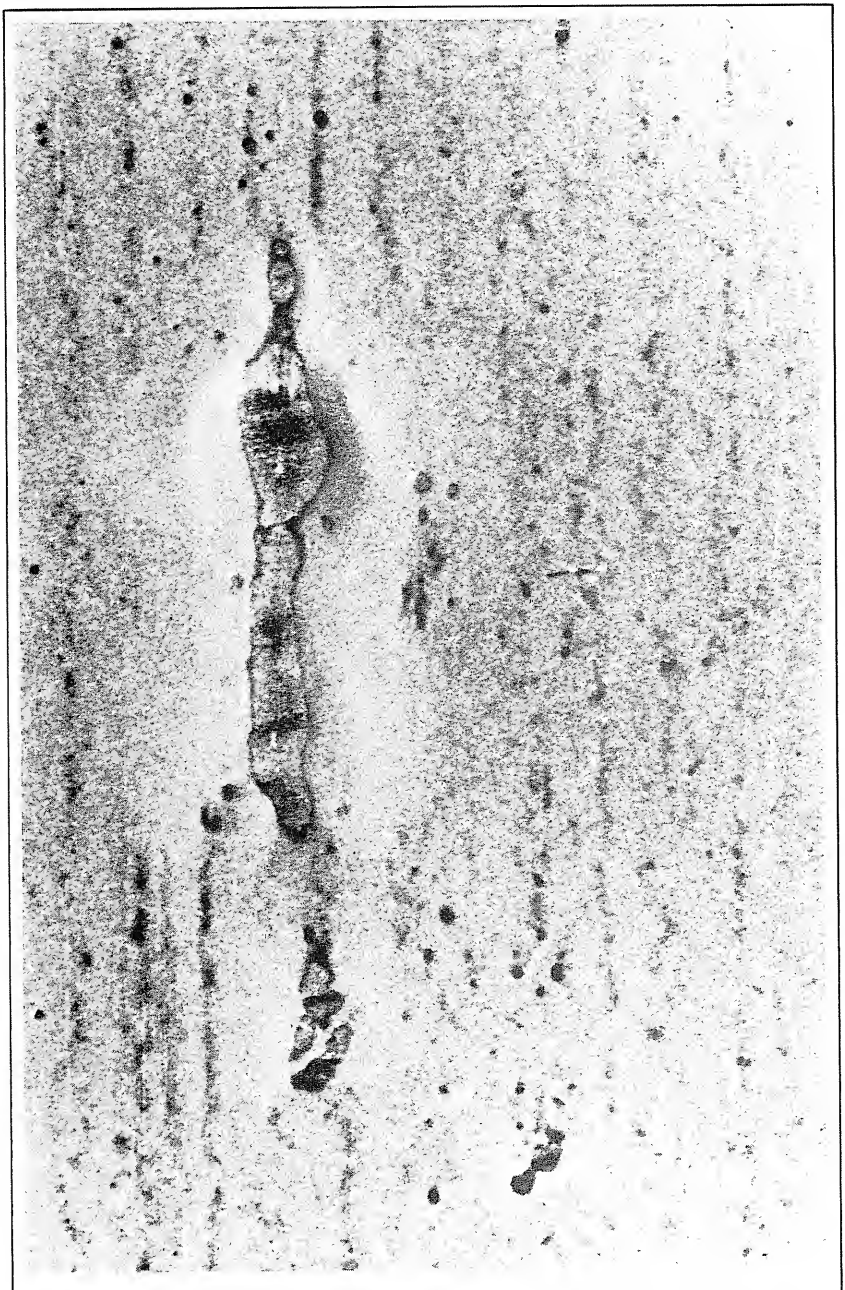


Figure 8.7: Tape Non-Uniformity Repaired

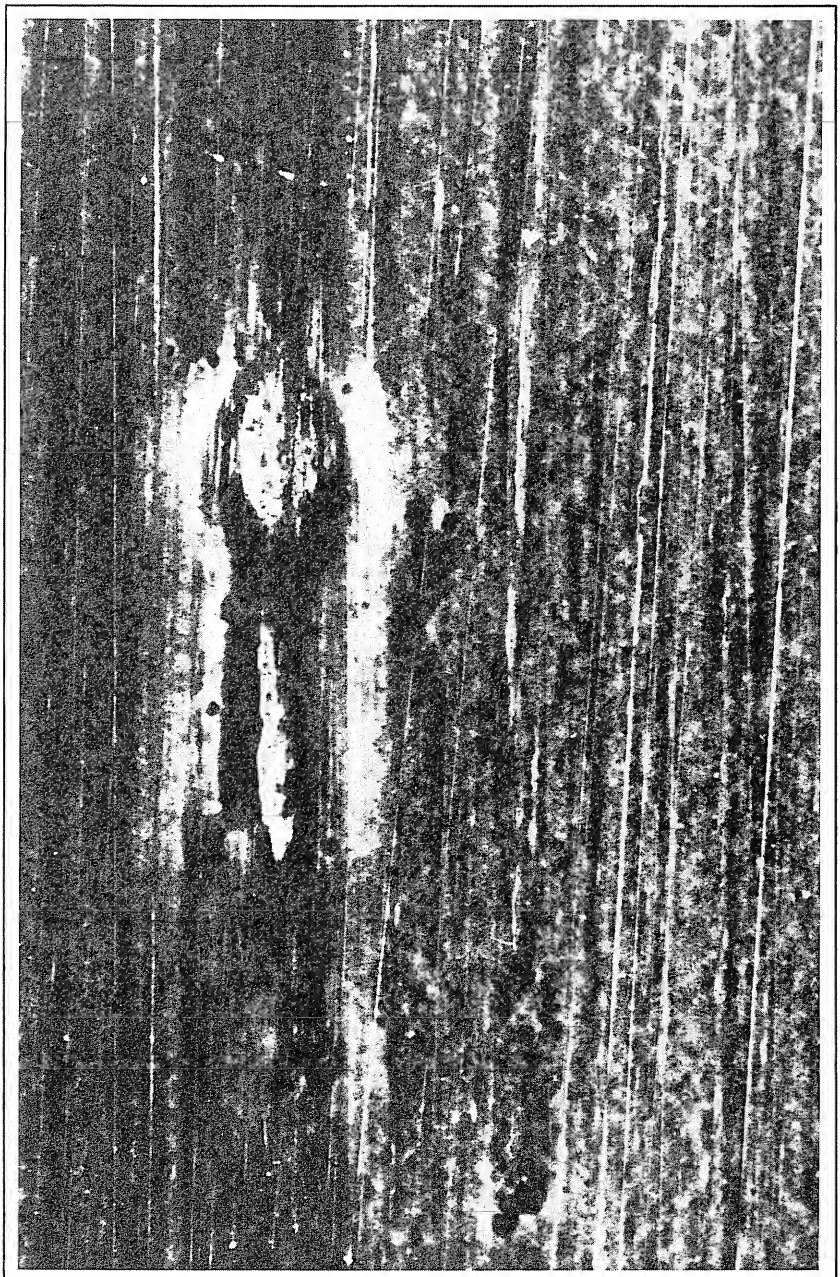


Figure 8.8: Tape Non-Uniformity after 100 Passes on Tape Drive

MAINTENANCE

Tape drives should always be kept clean. Head crashes are possible, just as with disks. In particular, a tape which is lifted 0.001'' from the head will cause a loss of signal. The recording and reading heads should be cleaned periodically. They can be cleaned easily by using a lint-free cloth or a piece of cotton lightly impregnated with freon or isopropyl alcohol and attached to the end of a wood or plastic stick (never use metal). You need only a moderate quantity of alcohol, and you should not allow the alcohol to come in contact with other parts of the mechanism. As a general rule, tape heads should be cleaned after every 8 to 10 hours of use. Check the manufacturer's recommendation, as some special tape heads may require specific solvents.

The rollers, hubs and any other guides or mechanical parts of the tape drive system should also be cleaned. They can be cleaned with a lint-free wiper. Solvents should be used with great care and only in accordance with the manufacturer's recommendations. In the case of an IBM type tape unit, the take-up reeel should also be cleaned to remove dust or oxide residue. (See Figures 8.9 to 8.12.) Also inspect and clean empty reels before winding tape on them for storage.

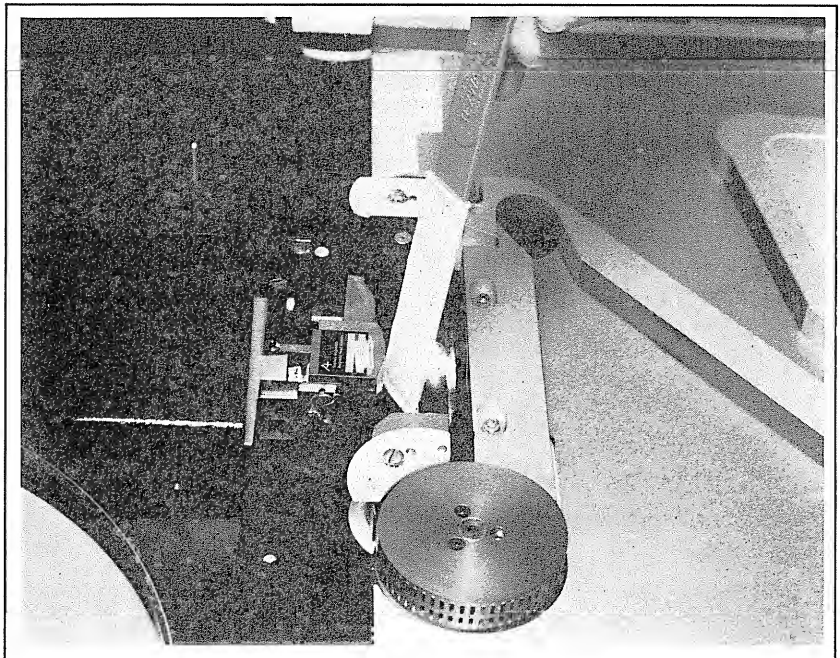


Figure 8.9: Cleaning the Head with a Special Wand

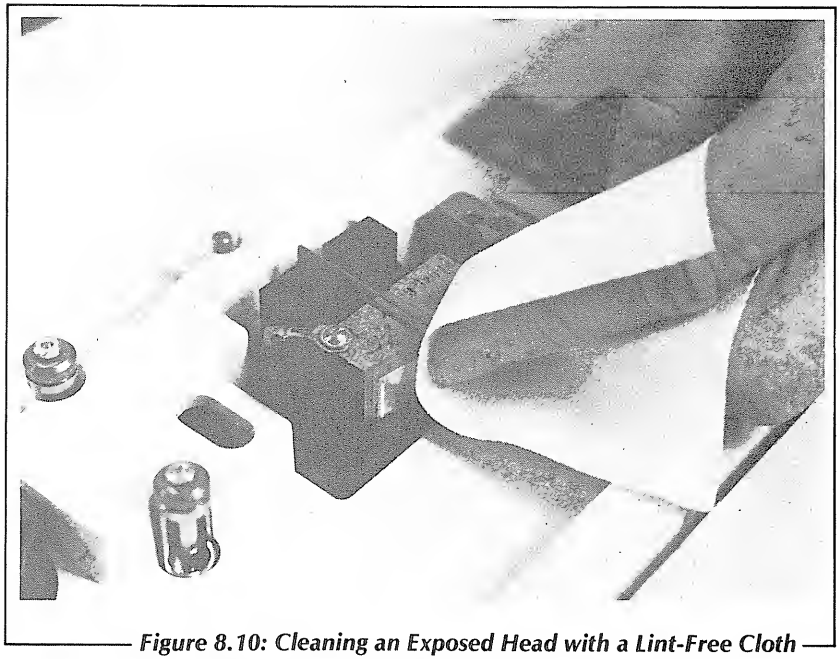


Figure 8.10: Cleaning an Exposed Head with a Lint-Free Cloth

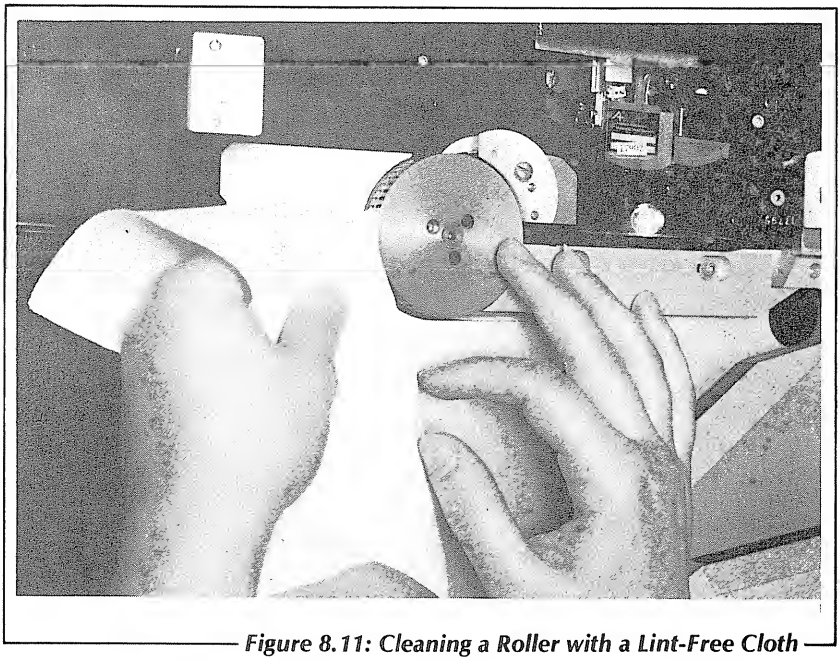


Figure 8.11: Cleaning a Roller with a Lint-Free Cloth

Figure 8.12: Cleaning a Roller with a Special Wand

As a rule, inspect the tape mechanism for dust contamination after each reel of tape has been removed. In particular, check the heads, rollers and guides, as these are the places where the greatest accumulation of particles is likely to occur. Cracked edges or other tape defects will result in immediate contamination of your mechanism.

Whenever a reel or a cassette is contaminated, discard it. This problem is *contagious*: The contaminating matter will get on the read/write head and contaminate another tape.

TAPE UNITS SUMMARY

Magnetic tapes are economical, robust, easy to use, and almost maintenance free. Treated with care and respect, they will give years of trouble-free operation. The main recommendations apply to the respect of their physical integrity. Maintain a dust-free environment and carefully inspect the tapes as well as the drives each time they are used.

CHAPTER 9
THE COMPUTER ROOM

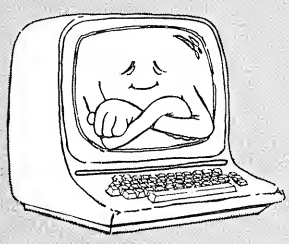
Caveat emptor.
Let the buyer beware.
—Latin Proverb

FOR THE HOME COMPUTER USER

No special computer room is required. A home computer can generally be plugged into a standard outlet and will operate well as long as reasonable precautions are taken: clean power, no extremes in temperature, no static, no dust.

The main recommendation for a simple home computer system is:

> *Keep the room comfortable for a human.* Your computer will like it too.



INTRODUCTION

Traditionally, large computers have been installed in specially designed, well-guarded computer rooms designed to protect such an investment and to insure reliable operation. Today's small computers, however, no longer require such a strictly controlled environment and are often installed in offices, homes and even factories.

Progress in integrated circuit technology has drastically reduced the number of components required to assemble a complete computer and has relaxed the environmental requirements. The smaller number of components has reduced the power consumption and the heat dissipation, decreased size, and increased reliability. Thus, most small computers and their peripherals can now be plugged into ordinary outlets in regular rooms or offices, and operate satisfactorily.

As long as basic precautions are taken such as providing clean power and a clean environment, small computer systems no longer require the elaborate precautions of larger computers. However, problems or inconveniences may arise. The purpose of this chapter is to describe the ideal computer room, i.e., the planning that should be done, and the precautions that should be taken, as well as the proper procedures that will insure the highest level of reliability.

The recommendations presented here should be examined in light of your working environment, the configuration of your computer system, and the degree of reliability required. You can then decide which steps are necessary and worthwhile for you. We will cover six topics in turn:

1. *Floor Planning*: The equipment, including cables, must be positioned properly within the computer room for secure, reliable, and convenient system operation. The specific requirements that apply to each peripheral will be discussed, as well as pre-delivery planning.
2. *Electrical Power*: The proper power quality must be supplied. This includes outlets, grounds, conduits and regulation devices.
3. *Environment*: Temperature, humidity, dust and static must be controlled.
4. *Furniture*: Appropriate furniture is important for reliable operation as well as for operator convenience.
5. *Fire Protection*: Fire protection requires careful advance planning and procedural precautions.

6. *Procedures*: Once the proper environment has been created for the computer system, the user or the operator must be taught how to use the system properly.

FLOOR PLANNING

The proper planning of a new computer installation is conditioned by three key factors: understanding the device requirements, making plans in advance, and laying out cables and interconnections properly. Let us examine them in turn.

Device Requirements

A typical business system consists of a central computer, one or more CRT terminals, one or more hard disk units or several floppy disk units, and one or more printers. Additionally, it may have one or more tape drives, a modem (for communications over telephone lines) and other accessories. Adequate space must be provided for these units. In addition, an operator work area should be provided in the computer room, and space should be allocated for the furniture necessary for storing supplies, tapes, disks, and manuals.

When preparing a floor plan for your computer room, you should consider the following factors: operator convenience, ease of access for maintenance, secure system operation, and operator safety. Naturally, the room must be large enough to accommodate all of the necessary equipment and furniture, and it must be equipped with a proper ventilation system. Let us first examine where each item of equipment must reside and what specific furniture, if any, it requires.

The computer proper must be located close to the disk units. This is necessary because the high-speed data transfers between the CPU and the disk require short cables. All other input/output peripherals, such as the CRT terminals and the printer, can be located at a distance from the computer itself. Our first space requirement is, therefore, to allocate a block of space for the computer-disk(s) combination.

In practice, it is usually convenient to keep one CRT terminal, called the console, close to the computer. This is particularly true if the computer is equipped with floppy disks, since commands must be typed at the console while disks are being changed. It is also convenient to locate the printer close to the console since, in order to print business forms, it may be necessary to repeatedly type a command at the console while aligning the paper on the printer.

CRT terminals intended for remote operators and users can be located almost anywhere in the building up to a distance of about 100 feet. As a final consideration, two items of equipment create high noise levels: the printer and the hard disk drive (with the printer being the worst offender). When placing these units, special consideration should be given to the noise that they generate.

In summary, the central processing unit, the disk units, the main CRT console, the printer and any tape drives are located in close proximity to each other in the computer room. Remote CRT terminals are normally located outside of the computer room throughout the office space. In special cases where the printer is particularly noisy, it may be located in a separate room, preferably equipped with a glass door or partition, for continuous monitoring. Let us now examine the furniture required by this equipment. We will then discuss site planning before the arrival of the equipment.

Furniture

The computer proper may be placed on an ordinary desk. Often it is inserted into a special desk or into a manufacturer-designed console that integrates not only the computer itself, but also the CRT terminal and the disk units. This design generally reduces the floor space requirement and improves operator convenience.

Hard disk units are either freestanding, mounted in an equipment bay, or placed on top of a desk. They must be carefully guarded against vibrations and shock, and a special manufacturer-provided enclosure is normally supplied. Allow for convenient, secure and safe storage of the disk packs or disk cartridges in the computer room.

Floppy disk drives are generally integrated within the computer cabinet or reside in a separate enclosure located close to it. Disk drives may be placed on top of a desk. The most convenient placement, however, is generally just underneath the desk surface so that diskettes may be inserted and removed conveniently without taking up work space on the desk.

When using floppy disk units, remember that a vertical storage rack for diskettes should be available and located close to the floppy disk drive, or else the operator may be tempted to leave the diskettes lying flat on top of the equipment. You can use a table-top rotating storage rack,or store diskettes in vertical plastic file folders inside a regular desk drawer.

Printers may be freestanding or table-top. High-speed printers must always be installed on a stable pedestal. If placed on a table or a desk, it is important to check the stability of the furniture during operation. Ordinary tables or desks are usually not suitable for high-speed printers for two

reasons: vibrations will affect the printer and paper jams are likely to occur since boxes of paper have to be located in front of and behind the printer. A specialized stand or pedestal is always recommended. Boxes of computer paper are best stored *outside* the computer room as they generate debris dangerous to disks and tapes. Other printer supplies such as fuses, ribbons and printing elements are best stored within the computer room.

CRT screens are table-top units. They may be located anywhere; however, for operator convenience, they should be installed on a low working surface. They do not require any specialized furniture.

Each item of equipment should be placed close to its respective power outlet. In addition, a secure path must be provided for the required interconnection cables. Also, each piece of equipment requires front access by the operator. In addition, most require *back access* for normal operation or maintenance. Many also require side clearance. These clearance spaces should be taken into account when planning the floor layout. They are called *service areas* and are discussed below.

Advance Planning

When planning for the arrival of a business system, the recommended procedure is to begin by making a scale drawing of the room that will receive the equipment. Then cut out rectangles or other shapes of paper that represent each piece of equipment drawn to scale. Each rectangle should allow for the area occupied by the device itself plus any front, back, or side clearance which is required or recommended. On each piece of paper, write the name of the equipment or furniture it represents, or make a rough sketch of it. Then, arrange the rectangles of paper on the room plan and see whether or not the arrangement is logical. When positioning the devices, keep in mind operator convenience. For example, floppy disk units are usually positioned on the right of the CRT terminal so that diskettes may be inserted or removed with the right hand. Similarly, the storage cabinet for diskettes is usually located on the right of the operator as well.

Also, make sure that the power outlets are properly positioned so that each piece of equipment may be plugged directly into its outlet.

Don't forget the operator working space and the storage cabinets in your plan. Disks and tapes should be stored in the same room as the computer so that no temperature equalization is required prior to their use. Manuals and essential supplies such as fuses and ribbons should be stored close to the related equipment.

A planning guide with typical equipment characteristics is shown in Figure 9.1.

A telephone should be installed in the computer room. It is an important

tool during diagnostics and maintenance. The maintenance personnel may work on the computer or other peripherals while simultaneously receiving instructions from the manufacturer or a service representative over the telephone. However, remember to position the telephone far from your floppy disk drive since a telephone ringing on top of a disk drive is likely to damage the diskette beneath it. Ideally, the telephone cord should be short enough so that it is not possible for an operator to inadvertently place it on top of the disk drive.

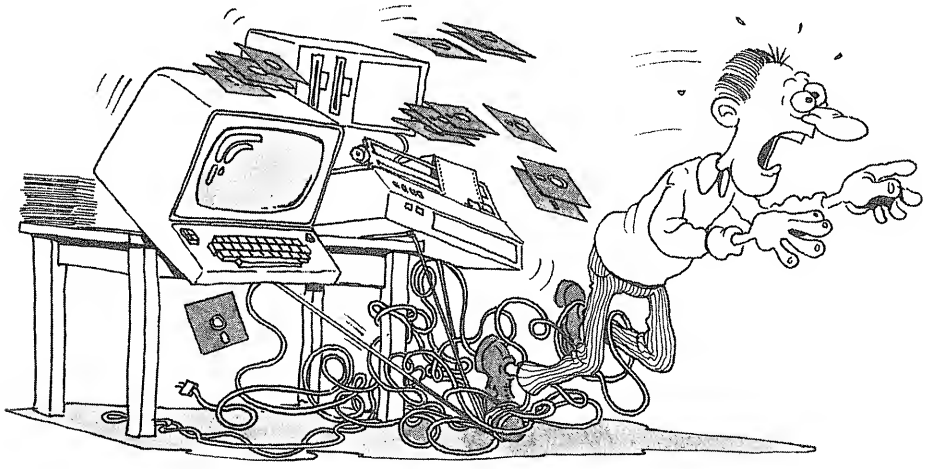
In addition, if you plan to transmit data over telephone lines, a modem and, of course, a telephone line will be necessary. If high-speed transmission is required, a special data line should be ordered in advance. A regular telephone line will accommodate transmission speeds of up to 4,800 baud but it is recommended that no more than 2,400 baud be used for reliable transmissions.

Finally, when positioning the equipment, put the piece of equipment that has the largest heat dissipation closest to the air-conditioning outlet so that it will remain cool.

If your printer is particularly noisy, special sound proofing may be required. In extreme cases, it may be necessary to put the printer at the far end of the room and enclose it behind a glass partition. If you should isolate the printer this way, always use a glass partition so that the operator may watch through the window for paper jams.

ITEM	WATTS	BTU	AMPS
PROCESSOR	250-500	800-1600	5-10
CARTRIDGE/DISK (fixed)	350-450	1200-1600	4-8
FLOPPY DISK	200	800	6
IBM TAPE	300-600	1000	5-7
PRINTER	300-800	1000	5-20
TERMINAL	150	500	5

Figure 9.1: Equipment Planning Guide



Routing The Cables

If certain items of equipment, such as the printer or the CRT terminal, are located away from the main computer, remember that the interconnection cables must be routed through secure and safe paths. Whenever this can be prevented, cables should not be left to lie on the floor. In an office environment, it is usually easiest to route long interconnection cables through the ceiling whenever space exists between soundproofing tiles and the actual masonry of the building. When such a procedure is used, the electrician should be told to avoid routing the cables next to power lines, light fixtures, powerful coils or transformers. In particular, interconnect cables should not be routed close to fluorescent fixtures.

Alternatively, cables can be routed through special ducts installed along or through the walls. In such cases, the cable should not share a common conduit with the power lines. The power lines may interfere with the proper operation of the interconnect cable. Finally, cables may be routed on or underneath the floor surface. In cases where cables *must* lie on the floor, they should be taped securely so that no one will trip on them or dislodge them.

As a practical recommendation, if you expect to use various cables or if you plan to disconnect or reconnect some units to or from your system, clearly label all cables. Many cables look alike and are terminated by identical connectors, however, their internal wiring may differ substantially.

Planning Summary

In summary, plan the computer room layout with care for proper system operation and operator convenience. A planning checklist is presented in Figure 9.2. As a general rule, the area available to the computer system should be four to five times the size of the area required by the equipment itself.

- ☐ SUFFICIENT ROOM AVAILABLE
- ☐ ELECTRICAL CIRCUITS INSTALLED:
  - ☐ OUTLET FOR ____VOLTS ____AMPS ____RECEPTACLE
  - ☐ OUTLET FOR ____VOLTS ____AMPS ____RECEPTACLE
  - ☐ OUTLET FOR ____VOLTS ____AMPS ____RECEPTACLE
- ☐ FURNITURE OR PEDESTALS FOR EQUIPMENT
- ☐ OPERATOR FURNITURE
- ☐ POSITIONING OF OUTLETS AND EQUIPMENT
- ☐ SPACE FOR ACCESS AND MAINTENANCE
- ☐ CABLES OF SUFFICIENT LENGTH (pre-installation may be required)
- ☐ PHONE LINE
- ☐ ADDITIONAL LEASED DATA LINE (for modem)
- ☐ STATIC CONTROL (floor covering/spray/mat)
- ☐ HUMIDITY/TEMPERATURE INDICATORS
- ☐ SUFFICIENT AIR CONDITIONING
- ☐ SUFFICIENT SOUNDPROOFING
- ☐ MINIMAL SUPPLIES
- ☐ STORAGE CABINETS

Figure 9.2: Planning Checklist

ELECTRICAL POWER

In a business environment, it is important to provide a separate power line for your system. In addition, the quality of the power delivered to the system may have to be improved. The power requirements of each unit have already been described in the corresponding chapters. It has been stressed that electronic circuits are sensitive to fluctuations in the power line and that transients must be eliminated prior to reaching the equipment. These recommendations particularly apply to users located in heavy commercial or industrial areas, during peak hours of electricity usage and during storms. This topic was addressed in detail in Chapter 5.

We shall now summarize the planning requirements for the reliable operation of a computer system. First, let us make an exception for home computers. We have already stated that a home computer system can usually be plugged into an ordinary household outlet and will function satisfactorily. It may fail, however, if an electric heater or a coffee maker is turned on in the house. Home-type systems, however, tend to be used in residential areas at night when the power is stable and when few appliances are being used, so that the quality of the electrical power available at that time is high. Further, an interruption is not catastrophic. This approach, however, is not acceptable in the case of a business or scientific system. Specific precautions must be taken. Let us systematically review these requirements.

The Outlets

Outlets must be located in close proximity to the equipment that they power. A separate, neutral ground is required for all computer equipment. This ground must be isolated from the conduit ground (the safety ground). It requires the use of a third wire and reduces electromagnetic interference and ground currents. Special receptacles are required of the Hubble or Slater types. Examples are shown in Figure 9.3.

Grounds

Each device requires:

- two phase conductors
- an insulated (green) wire as the reference or frame ground that reduces susceptibility to radio frequency (RF) currents, static discharges and fluorescent lamps

- an AC neutral or safety ground, important for personnel safety in case of lightning or a short. This wire is also called common and AC return and is white or light gray. It normally carries no current.

The system must operate with a single, common ground located at the power distribution panel. The reference ground is then connected to the distribution panel frame or to the copper ground bus. Ground runs should be kept short since they increase the inductive reactance, resulting in a voltage differential and reduction in the efficiency of radio frequency interference (RFI) filters.

The voltage differential between the reference ground and the safety grounds should not exceed plus or minus 2 volts at 117 volts AC. When 220

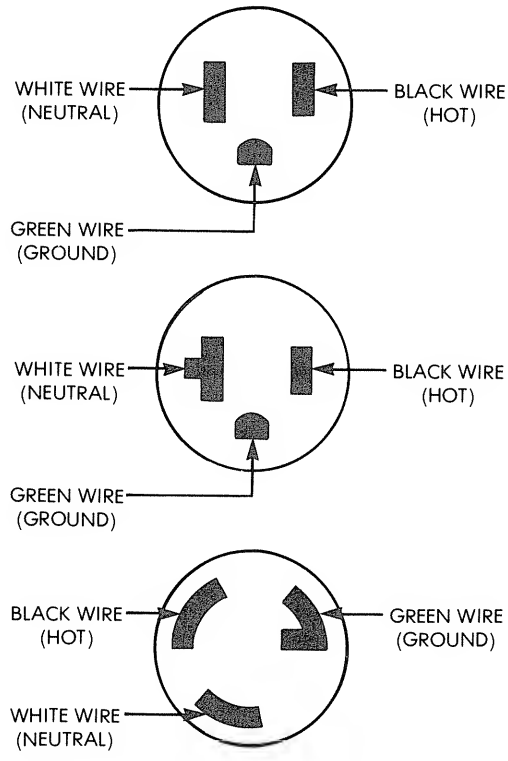


Figure 9.3: Typical NEMA Receptacles

volts are used, breakers and/or fuses are recommended for high current surges.

Conduits

All conduits must be insulated from each other in order to prevent ground loops. Bare wires should not be allowed to rub against each other or against a conduit.

Lightning

Lightning arrestors should be installed outside the building, close to the power source.

Using The Outlets

Once single-line, dedicated circuits have been installed for your computer equipment, don't defeat their purpose by plugging other equipment into these circuits. In particular, don't plug in an office machine, heater, copier, air conditioner or coffee pot. This is why it is a useful precaution to also have "ordinary" outlets available in the computer room. Unused outlets on the computer's dedicated circuit should be capped in order to prevent anyone from plugging other equipment into them.

Circuit Breaker

A separate circuit breaker for the computer room is recommended so that power can be turned off in case of an emergency.

Line Conditioning

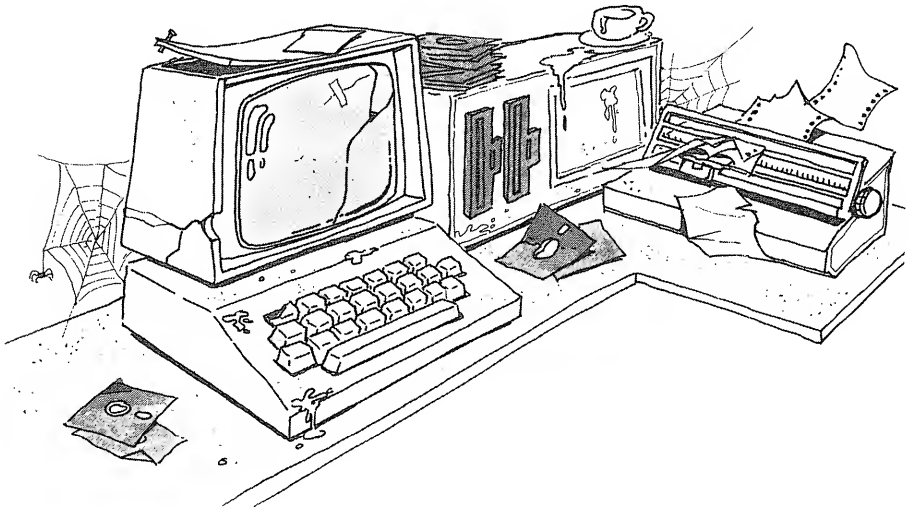
A surge protector or even a line regulator may be required to provide clean power. In particular, when a dedicated line is not available, use at least a line isolator with surge protection. This low cost device will provide a degree of protection against fluctuations and surges.

THE ENVIRONMENT

The specific environmental requirements for each item of equipment have been described in the corresponding chapters. We will summarize the main requirements here. A comparative table is shown in Figure 9.4.

In general, what would be considered good basic working conditions for a human operator will satisfy most computer systems. Specifically, this means suitable air quality and temperature, no dust or pollution, sufficient

humidity, and the absence of direct sources of heat (such as large windows). In addition, static must be avoided. Let us examine each of these requirements.



STORAGE SUMMARY			
ITEM	TEMPERATURE °C	°F	RELATIVE HUMIDITY (%)
FLOPPY DISK	4 to 43	39 to 109	8 to 80
HARD DISK	10 to 50	50 to 122	8 to 80
MAGNETIC TAPE	15 to 50	59 to 122	20 to 80
PRINTER PAPER	10 to 43	50 to 109	30 to 65
ALLOW 24 HOURS TO EQUALIZE			

Figure 9.4: Environmental Requirements for Storage

Air Quality

Ordinary filtered, recirculated air conditioning of the type provided in most offices is sufficient for most computers. Air conditioning is usually required for hard disks. It may be necessary, in some cases, to install an additional air-conditioning unit in order to satisfy this requirement. The filters must provide at least 90% efficiency with standard test dust. A higher efficiency may be required in a high pollution environment, such as a production area or an office where dust is generated by the professional activity (for example, a dental office). It is best to have independent temperature control for the computer room in order to guarantee that the proper temperature will be maintained automatically. If this is not possible, try moving one of the sensors of your air-conditioning system within the computer room to guarantee that the proper temperature limits will not be exceeded in that room. If this does not work, install a separate air-conditioning system.

Temperature Control

Heat is generated by the working equipment, people in the room, light fixtures, windows, and air circulation. Temperature should be kept between 15° to 26°C (60° and 80°F). The gradient of temperature change should not exceed 8°C (15°F) per hour.

In rooms with large windows, the use of drapes or other shades is recommended. Always avoid direct sunlight in the computer area as it might damage diskettes and tapes, as well as raise the operating temperature of the system.

Static Electricity

The buildup of static electricity must be strictly prevented in order to prevent transients or direct damage to integrated circuits or magnetic surfaces. Remember that in a dry environment, just a few steps across a room can result in a static discharge of 5,000 to 15,000 volts or more. The buildup of static is encouraged by materials such as nylon rugs, insulating soles, and a low relative humidity. There are three main remedies against static:

1. Keep the humidity level at 50% or higher.
2. Avoid all types of carpeting, but especially regular nylon carpeting. If you have nylon carpeting, remove it.
3. Use anti-static mats and sprays to reduce static.

To reduce static, the installation of a tile floor rather than carpeting is

strongly recommended. The maximum resistance between the floor surface and the building floor should be on the order of 10^{10} ohms. When using tiles, their resistance should be 0.5 megohms to 20,000 megohms at 40% to 60% relative humidity and 18° to 24°C (64° to 75°F). Avoid asphalt tiles that chip easily and create dust. Use vinyl or better still, laminated fiber resin. For floor maintenance, avoid standard wax: It increases resistance. Only use specially designed high-conductivity waxes.

If carpeting is required, use an anti-static type. Anti-static carpets typically incorporate metal fibers as part of the material and are easily recognizable. The maximum static buildup for such carpeting should not exceed 2 kilovolts.

Furniture used in the computer room should have a conductive contact with the floor. This can be achieved with metal legs, or when casters are used, with metal rather than plastic casters. The resistance between the furniture and the floor should be less than 10^9 ohms. Don't allow rubber wheels or feet for the furniture.

Relative humidity within the computer room should be from 40% to 80% non-condensing. This will eliminate most static-buildup potential. The ideal relative humidity is 50%, and the equipment will accept 20% to 80% relative humidity. However, whenever the relative humidity falls below 40%, static becomes a danger. The gradient, i.e., the rate of change, should be no more than 10% per hour.

Anti-static sprays may be used where static is a real danger. However, these sprays present two main disadvantages. First, over time they will corrode the equipment. When applying anti-static spray, make sure that all of the equipment is turned off. Don't spray in close proximity to any electronic equipment. Second, anti-static spray is only a temporary measure and will work for only a few weeks or months at most. It must be reapplied regularly.

If the room is carpeted, or if static is detected, use anti-static mats. At least one mat must be used beneath the chair in the working area (see Figure 9.5). Tufted mats may be used (they dissipate the charge within the mat), but grounded mats are better (there is no residual charge). When using a grounded mat, the cable should use a high resistor (1 megohm) to prevent shock danger to the operator in case a large voltage should appear on the ground circuit. Additional mats may be required at the entrance as well as in front of each unit.

In summary, remember that any static discharge at 3 meters (10 feet) or less is dangerous: Electromagnetic fields are radiated and noise is conducted. Never cause a direct static discharge on any cabinet, including the CRT keyboard and the printer. If the static danger is high, use only conductive shoe soles (leather soles are recommended).

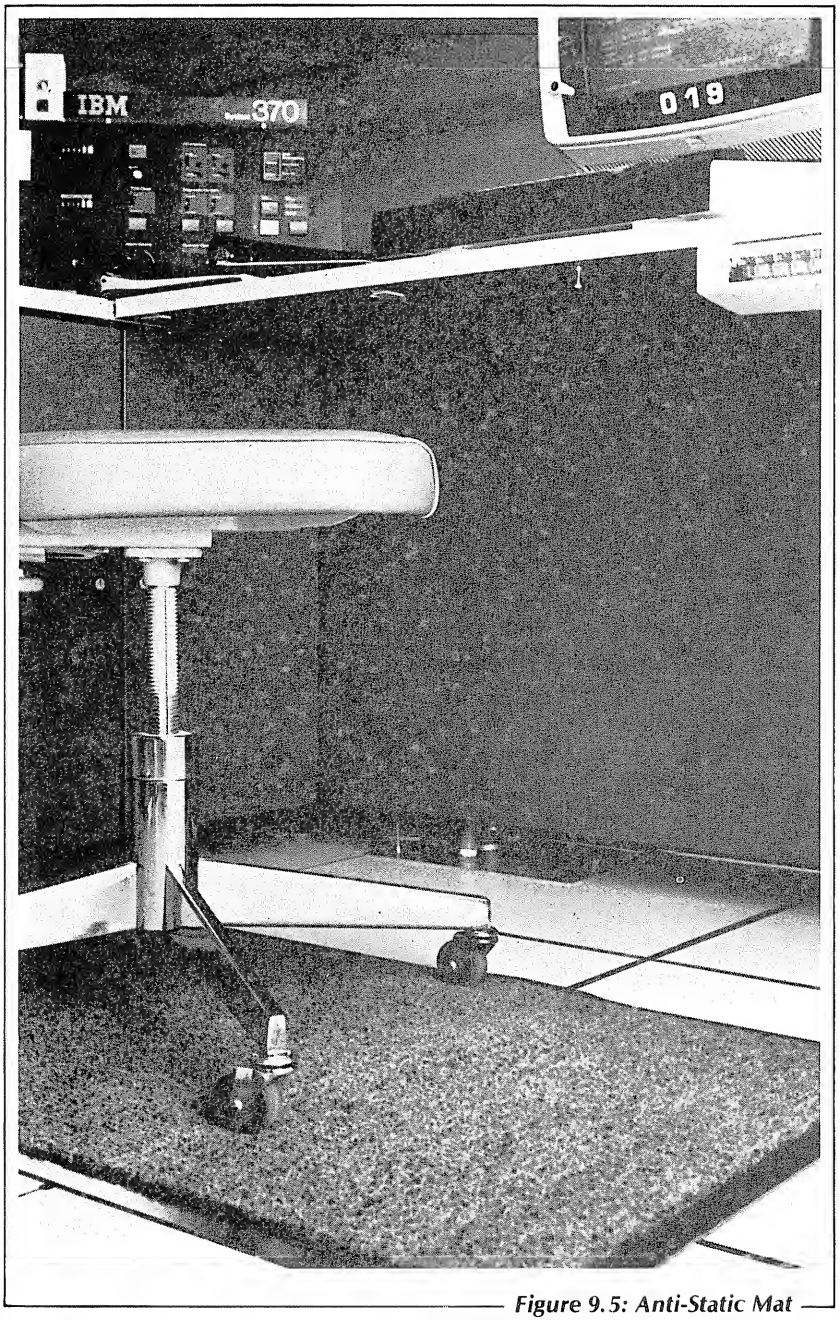


Figure 9.5: Anti-Static Mat

Dust and Liquids

Don't let dust or liquids come in contact with the computer equipment. It is best to disallow all liquids from the computer room. In addition, if a hard disk or a tape drive is used, it is best to disallow all smoking within the computer room. Sustained smoking in close proximity to a disk or tape drive will contaminate it. However, the likelihood of damage to a diskette is less than to a hard disk or tape.

Consider the following measures in order to keep dust out of the computer room:

- Seal all windows.
- Reduce traffic through the room.
- Keep coat racks outside the room.
- Don't allow your janitorial service to enter the computer room. Use a special lock.

FURNITURE

We previously described the basic furniture requirements when planning the computer room. Let us now examine the function of each item, as well as its proper use.

The furniture used in the computer room should be sturdy, convenient, and sufficient. Equipment and furniture used to support heavy items should be sturdy. This applies, in particular, to printer stands.

The furniture used in a computer room should also be convenient to use. For example, CRT displays should be installed on low stands or tables whenever possible. Storage drawers should be available in close proximity to floppy disk drives. Finally, the furniture selected should be sufficient for all of the needs of the computer room.

In particular, in addition to the furniture required by the equipment itself, additional furniture must be available for the following purposes:

- A work area, equipped with a table or desk, and preferably a telephone, should be provided. This work area can be used by the operator or maintenance personnel when consulting maintenance manuals, or simply in the course of work assignments. It is best located away from the computer equipment so that no pencils, paper clips, or staples may fall into the equipment. The telephone line should be located away from the disks so that accidental damage to the disk by a ringing telephone is avoided.
- Furniture should be available for storing the required documentation, magnetic media, and supplies. The documentation should

always be complete and readily accessible. Usual supplies such as paper, ribbons, and printing elements should also be available. However, specialized business forms, such as invoices, statements, and checks should naturally be kept in a secure location, usually locked.

- Magnetic media, such as disks, diskettes, and magnetic tapes should be stored in racks or containers, in closed metal cabinets. Remember that disk cartridges and tapes should be stored vertically in specialized racks; they should not be stacked on top of each other. Blank disks and tapes should be stored separately from those that contain data. In particular, backup disks and tapes containing valuable business information are best kept in a locked cabinet. It is best to store all software required to operate the computer as well as blank disks and tapes, within the computer room itself, so that they remain at the same temperature as the equipment. However, backup disks and tapes should be stored outside the computer room, at a separate site, preferably in a fire-safe cabinet or in some other safe and secure environment. Secondary backups may be left in the computer room, if necessary. They will be less secure, but they will provide operator convenience.

It is important to understand the function of such additional furniture in the computer room, and to plan for it in advance, so that the furniture layout will allow for easy operator access to the required supplies or filing cabinets.

As a final recommendation on equipment, when cleaning don't use a vacuum cleaner with a metallic nozzle, since it may affect magnetic devices as well as scratch fragile surfaces.

FIRE PROTECTION

Fire is always a danger wherever electrical machines are used. Many fire hazards exist with computer systems:

- metallic objects, such as paper clips or loose screws, dropped within an enclosure, causing a short circuit
- obstructed ventilation outlets on cabinets, causing internal overheating
- bare wires causing a short circuit
- a paper jam causing over heating

- a disk head-crash causing destruction of the head and/or the platter and subsequent short circuits
- liquids or condensation over printed circuit boards causing burn-outs.

Always assume that a fire can occur, and plan for it. Plan for the security of the installation, including the data, as well as for the safety of the personnel.

Don't use water on an electrical fire. If a sprinkler system is used, use a dry pipe, or better still carbon dioxide (CO_2) or hydrocarbon bromide ("halon"). Provide fire extinguishers that use either carbon dioxide or halon for small fires.

A word of caution: carbon dioxide is effective on the equipment, but it is a safety hazard, as it asphyxiates people by oxygen deprivation. If carbon dioxide is used, all personnel should be out of the room within thirty seconds. An audible alarm must be provided.

Halon 1211 works well on the equipment and is considered to be non-toxic. Halon is non-conductive, works at a safe temperature ($-10°C$ to $-5°C$, i.e., 15° to 25°F versus $-73°C$, i.e., $-100°F$ for CO_2) and does not leave a residue. It is, therefore, currently considered to be the best. Halon extinguishers are shown in Figure 9.6.

Figure 9.6: Halon Extinguishers

As additional precautions, clear the computer room of paper stacks and other flammable material, and install smoke detectors. In case of emergency, first cut off the electrical power (we have already indicated the need for a separate circuit breaker at the entrance of the computer room), and then try to save the records if reasonably possible. We have already stressed that all original programs and backup copies of all data must be stored in a *separate* location, away from the computer room, preferably in a separate building.

Now that the computer room is properly installed, furnished and ventilated, let us use it properly.

PROCEDURES

Whenever a computer system is used for business purposes or is used by several operators, it is imperative that all operators be aware of the proper operating procedures, or you will be a victim of the "time bomb" phenomenon. One of the operators will damage the system in some subtle way and the malfunction will be detected only much later, thus making it difficult or even impossible to determine what caused it.

By insuring that the proper procedures are followed you can prevent harm to the system, as well as to the files or the business itself. Let us first examine the basic rules to follow, then the precautions that apply to security and confidentiality.

Basic Rules

Two essential rules are:

1. Train all operators in the proper use and operation of each device of the system (as explained throughout this book).
2. Keep a system log in the computer room. The system log may be a simple 3-ring binder or perhaps a more formal log with non-removable pages. All malfunctions, maintenance operations, and equipment modifications should be logged in this book. In short, any intervention on the system hardware must be properly recorded. Indications of important software changes would also be useful. Whenever an incident occurs, proper documentation is essential for a correct diagnosis and should include the best possible description of the symptoms and an evaluation of the environment at the time that the error occurred, including exceptional conditions such as high temperature, the presence of a large number of people in the room, or the use of new software.

Here is a horror story to stress this recommendation.

A new printer was installed at Company X. Sometime later, one of the technical persons remarked that this printer could be made to operate at a higher speed. It merely required a small re-wiring inside the printer, which could be achieved by a jumper on one of the boards. However, another clever technical person found that the same effect could be obtained by wiring together two contacts just behind the front panel of the printer. This arrangement worked fine for several weeks. Eventually, software was installed on the system, that required the lower operating speed for the printer. The printer was inspected and since no jumper was present on the board, it was assumed that it was operating at the lower speed. Unfortunately, for weeks, the printer did not operate properly with this new software. The entire system was extensively checked out. The software was replaced, but the system still did not operate properly. Eventually, after much time and effort, the printer was completely taken apart and, one day, the unusual connection behind the front panel was discovered. By this time, just about every part of the printer had been replaced.Cutting the "clever" connection behind the front panel resolved the problem.

Clearly, this problem could have been avoided if the unusual soldering had been properly recorded in the system log. Unfortunately, in the absence of the log, no one thought of the front panel possibility. In most computer environments, there will *always* be a clever person that will suggest or actually effect some clever change. If you allow this to happen, make sure that the nature of the change is properly recorded, so that you have some possibility of undoing it later, if required.

The main rules should be posted in a conspicuous place. At least they should include the basic DOs and DON'Ts about sensitive equipment such as floppies and other disks. Also, the telephone numbers of maintenance personnel, and the procedures to be used in case of malfunctions, as well as the location of usual supplies, should be clearly indicated.

Confidentiality and Security

Any skilled operator who accesses a computer system may be able to examine copies of any files within the system. Although many systems are equipped with elaborate security procedures and software precautions, a truly skilled programmer will usually be able to break through software barriers to get at the information that he or she wants. However, this does not mean that barriers against unauthorized access to confidential information should not be established.

The concept is the same as in providing security for a home or building. First, erect a reasonable number of barriers that will discourage people from gaining illegal access to confidential data. Second, advertise the fact that the system is protected. Many procedures may be used to that effect and are discussed in Chapter 12.

SUMMARY

Careful, advance planning of the computer room will result in reliable operation of your system as well as in a safe and convenient work environment. In this chapter, we have presented in detail the requirements of each device, and recommendations for laying out a suitable floor plan. We have stressed the importance of clean electrical power, a suitable environment, and appropriate furniture. We have indicated the need for fire protection and explained the basic procedures required for effective operation.

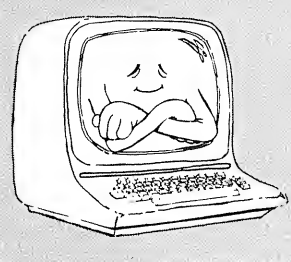
CHAPTER 10
SOFTWARE

I know a trick worth two of that.
— Shakespeare, King Henry the Fourth,Part i, Act II, sc. i., 40

FOR THE HOME COMPUTER USER

The main recommendation is:

Back-up any new software you receive and any new files you create.



INTRODUCTION

Software refers to all the programs used on your installation. Software can be classified in three general categories: the operating system, the languages, and the application programs.

The *operating system* provides you with the basic commands required to use the computer, as well as the peripherals (such as the disk unit and the printer). The operating system is generally supplied by the hardware vendor and is never changed by the user. However, the operating system, like all software, evolves over time, and the vendor will normally provide new versions periodically. Normally, all older programs and files can be used with the new version, but not always.

The *languages* include the interpreters or compilers for programming languages, such as BASIC, COBOL, FORTRAN, and Pascal, that may be available on your computer. Programs are written either in assembly language or in a high-level language. Programs written in assembly language can be directly executed by the computer. Programs written in a high-level language, such as BASIC, must first be translated into machine-executable code in order to be executed by the computer. This is the purpose of the language translators (interpreters and compilers).

If you need to execute a program written in BASIC, you need an appropriate BASIC interpreter or compiler in order to execute it. Even though many computer languages have been standardized, each *version* of a language is generally slightly different, so that you must use the exact version of BASIC that your program was written for. Thus, whenever a language compiler or interpreter is executed, you will see on the screen "Version 2.3" or a similar notice. It is important to use the right version, as your programs may not execute correctly with a different version.

The *application programs* are all of the programs that actually do something for you, such as word processing, accounting, mailing list, and games programs.

In this chapter, we will see that all programs have specific limitations and impose space requirements. We will discuss proper software maintenance, operational procedures, and the precautions relating to hardware and software changes.

SOFTWARE REQUIREMENTS

We will now examine the common requirements and dangers posed by programs. We will first discuss the impact and dangers of varying control

conventions. We will then look at the workspace requirements imposed by most programs, and finally we will examine the utilities that facilitate software use.

Control Functions

Each program, once it executes on the computer, has the potential to redefine the function of the keys on the keyboard and impose its own input conventions. For example, control keys as well as special function keys on the keyboard are normally used for issuing special commands to a specific program, such as: erase, backspace, move back, stop, or proceed. Different programs may use different conventions. Remember that special keys may have different meanings for different programs. Naturally the most dangerous functions are those that will abort the program or affect data files. The operator must be aware of the functions of the special keys and must be warned against the effects of "dangerous" keys. For example, when using a mailing list program, it is possible to hit a control key by mistake. The command generated by the control key may be neither interpreted nor rejected by the mailing list program. Instead, the spurious control character may be merely inserted in the address. Later, when this "contaminated" list is used, sorting or selection functions will generally fail because the presence of a control character will interfere with those functions, i.e., the control character is illegal.

Many programs are not completely protected against "wrong" inputs. If you are aware of specific dangers, be sure to warn all users and operators. This is particularly important in a business environment where input typists may inadvertently contaminate or even delete valuable business files. Similarly, when an older version of CP/M (a well-known operating system for microcomputers) is being used, inadvertently hitting a control-C, i.e., simultaneously depressing the "control" key and the letter C, may result in the loss of all input typed so far, or even the loss of a disk file. When such dangers exist, you may want to stick a red dot on the control key, or warn system users in some other way.

One more word of caution: Most programs provide an "escape" key that stops the program and returns you to the operating system. Beware of hitting this key because you will generally not be able to restart the program where you left off. In particular, if you are typing in text or data, and hit this key, the text or data will generally be lost, unless you preserved them on disk before exiting.

Remember that many input programs, such as word processors,don't always save information on disk automatically. The program usually accumulates text as it is typed in RAM memory. You must explicitly transfer the

contents of the RAM to disk. Do this frequently in order not to risk losing data. Specific commands are provided to this effect. Remember, if you use an "emergency exit," such as an escape, the RAM contents are generally lost.

Don't leave your word processor program abruptly. Use the proper exit command that saves the memory onto disk. Similarly, always save the contents of your RAM at regular intervals—just in case there is a power failure—or in case you leave your terminal unattended. In short, don't entrust any large amount of information to RAM. RAM is volatile. Save the information on disk as soon as possible, for example, at five or ten minute intervals, or whenever a page of text has been typed in.

WORKSPACE REQUIREMENTS

Each program requires a minimum amount of memory in order to be executed. In addition, it may require additional space on the disk. You must be aware of these requirements. For example, a 16K BASIC interpreter requires at least 16K of internal memory. To reduce the risk of errors, most *systems software* (i.e., operating systems and languages) are labeled with the required memory-size; and this size is also confirmed on screen. Thus, if you are using a 48K CP/M version (an operating system), and a 32K BASIC (an interpreter), the minimum amount of memory required by this combination is 48K (the largest requirement of the two programs).

Similarly, many programs require *workspace*, i.e., scratch storage space on the disk. In particular, programs that operate on files, such as editors, word processors, sorting programs, merging programs, or selection programs, generally require a work space at least as large as the file they are operating on. The best programs may still work with a smaller workspace, but they will execute much slower. Most others will stop in mid-course when they run out of disk space. For example, if you plan to sort a mailing list alphabetically, one of the disks must generally have an empty area that is at least as large as the file that you are planning to sort. In addition, some sorting programs may require that the workspace be available on a specific disk drive.

Similarly, some file copying programs require a workspace that is at least equal in size to the file that they are copying. This is almost always the case for editor and word processing programs that automatically create a backup copy of the file in case an accident should occur during the transfer. Typically, if you plan to use such programs, a safe solution is never to fill your disk beyond half of its capacity. However, this restricts the maximum number of entries on that disk. The operator should be made aware of

these limitations. They can be removed by adding an extra disk drive to the system.

When building a mailing list system, it is particularly important to be aware of the storage limitations of the disk itself, i.e., the maximum number of entries that the disk may accommodate. However, it is also important to be aware of the storage limitations imposed by the sorting and copying programs. Otherwise, a complete diskette may be filled up, and it may become difficult to remove half of the names on that diskette once it has become full.

Whenever a program that operates on files fails, first check to see if it ran out of disk space. The program itself might tell you this by displaying an error message such as "DISK FULL." If it does not, then check the size of the remaining disk space. If necessary, make room on your disk by removing nonessential files.

SOFTWARE FACILITIES

Many programs are available to perform common chores such as printing, formatting, data capture, text input, code conversion, and disk copying. Become familiar with the *utilities* provided on your installation, as they can save you much time. Here are some common facilities:

- A *word processor* or an *editor* allow you to type text conveniently, modify it and edit it.
- A *data-base program* is a special editor that structures your data into related fields and allows you to check the validity of input.
- A *report generator* allows you to conveniently print formatted reports from a given file or data base.
- A *file system,* generally part of the operating system, allows you to create, label and manipulate files.

When copying disks, there are special programs called *track-to-track copiers* that will make a complete copy of one disk onto another one and require no working storage. When an entire disk needs to be copied, a track-to-track copier will do it in less time than the usual copy program of the operating system.

However, when a *single* file on a disk needs to be copied, the file transfer program provided by the file system should be used. In the general case, it may also be advantageous to use a file copier program rather than a track-to-track disk copier, because a good file copier program will often copy successive blocks of information from one file onto physically adjacent

sectors of a blank disk. As a result, the new copy will usually require less time to be loaded into the system the next time around, since fewer sector searches will be necessary.

Many other utilities exist that facilitate programming, such as sorting programs, merging programs, disk editors, diagnostic programs, mathematical and other program libraries. Investigate the available resources before reinventing the wheel.

SOFTWARE MAINTENANCE

Over time, most software programs will require maintenance for two reasons. First, they all contain bugs or errors which (hopefully) are not detectable during normal usage. Second, over a period of time, the designer usually keeps adding features. Let us consider these two points.

Nearly all programs of any length contain bugs. This is because any human construction of large complexity, such as a machine, a car or a program assumes tolerances that are not always correctly evaluated, and includes design errors that appear only under exceptional circumstances. This is why it is best to use a business program that has been well-used and well-tested—by someone else, preferably—and by as many users as possible.

The maintenance task of debugging a program, i.e., removing errors, must be performed by the software supplier or designer. You should secure a suitable maintenance agreement prior to purchase of the software.

The second area of software maintenance lies in the improvements or modifications brought to an existing program. These changes may be performed either by the software vendor or by someone in-house.

If you decide to tailor a program to your own application, do so with the greatest precautions. Changes in a program should normally only be performed by the designer of that program. Another person performing changes in that program will usually introduce subtle bugs or errors, thus degrading the reliability of the system. Don't change a program unless you thoroughly understand it and can properly document the changes that you have performed.

In addition to the correction of bugs and other in-house changes, software maintenance normally involves securing the latest versions of a program from the software vendor on a regular basis. These new releases contain corrections of newly discovered errors as well as new features. In principle, most software suppliers will automatically keep you advised of new releases so that you can obtain them. In practice, it is best to verify at periodic intervals whether or not a new release is available. Thus, it is a good

practice to call the software supplier every six months and ask for information on the latest release. However, when obtaining a new release, make sure that all of your previous data files can be used with the new version.

SOFTWARE PROCEDURES

The four essential recommendations that apply to using a program and a data file are:

1. Label it.
2. Back it up.
3. Keep it safe and secure.
4. Document it.

We will examine each recommendation in turn.

Label It

As soon as new data or a new program is recorded on a magnetic medium, label it with the contents and date. Always make sure that you can identify the latest version, as well as important copies.

Back It Up

Any time a new program or data file is received, make a backup copy of it. Then, file the original away in a safe location, and use the copy. Similarly any time new data is created at the end of a working period, make a copy of it and store it in a secure location.

Keep It Safe and Secure

All magnetic media containing programs or data should be properly handled and stored in an appropriate storage container. In addition, confidential disks or tapes should be kept under lock and key at a secure location.

Keep Documentation Available

All the documentation required to use all of the software should be available in the computer room. It is crucial that this documentation be complete and up-to-date. You might want to mark the documents with special stickers that say "Do Not Remove," or to use some other method to obtain this result. Any lack of documentation is usually only detected

during critical times, such as diagnostic runs and malfunctions, and may have a serious impact. As an additional safeguard, it may be advisable to keep one extra set of documentation describing all common programs that are available, for consultation *outside* the computer room. You may want to announce this fact on the documentation cabinet. Hopefully, an operator will be less tempted to remove the indispensable reference document from the computer room itself.

HARDWARE CHANGES

Whenever new equipment is added to the computer system, some of the programs may require changes. Whenever a new peripheral is added to the system, the operating system must usually be modified to handle it, i.e., a new version must be installed. Whenever a CRT terminal or a printer is changed, programs that communicate directly with these terminals in a specified format may need to be changed. This generally includes, in particular, formatting programs and word processors. Be aware of the required software and hardware changes at the time that you decide to change peripherals.

SOFTWARE CHANGES

Typically, new software will continually be added to a system. Since the capacity of disks and tapes is limited, there will generally be a main system disk that is used at all times, that contains the most recent software in use on that system. In time, older software will be erased from disks and will become more difficult to find, unless you have a good labeling and archival system. Remember: as a strict and indispensable procedure, any time new software is received, a copy should be made. The copy should then be used by the operator, and the original stored in a remote, safe location. Then, whenever it is necessary to use a program that is no longer around the computer room, the original can always be found in the safe, backup location. Naturally, access to this safe, backup location should be strictly controlled, and, normally, operators should not have access to it. This will reduce the risk of inadvertently destroying or removing the single remaining copy of a program or data file.

SUMMARY

Operating and maintaining software requires some simple precautions that have been described in this chapter. Because there is no "standard software," additional precautions must be taken with specific programs.

For example, we pointed out that a mailing list file can be damaged by entering spurious control characters, and that a word processor file can be lost in part by exiting incorrectly. However, the greatest damage that can normally occur is to lose the contents of a file. As long as proper labeling and frequent backup procedures are used, this problem should be minimal and thus limit any loss to only a few hours work.

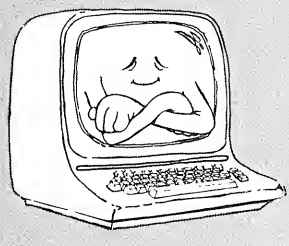
CHAPTER 11
DOCUMENTATION

Accuse not nature, she hath done her part. Do thou but thine.
— Milton, Paradise Lost, I, 561

FOR THE HOME COMPUTER USER

The main recommendation is:

Keep all documents and manuals readily available.



INTRODUCTION

Documentation is essential to the effective and convenient use of a computer installation. Documentation must be complete, current, easy-to-use, and well-organized. Three kinds of documentation must be available: hardware documentation, software documentation, and a record of changes or modifications to the hardware or software.

HARDWARE DOCUMENTATION

The recommendations presented here apply primarily to the hardware, but most are applicable to both hardware and software. Two types of hardware manuals should be kept at the installation site: user manuals and detailed reference manuals.

User manuals are required by the user because they describe the correct operating procedures and maintenance steps for each device, including the peripherals. The user may often need to refer to these manuals to find the steps to be taken in the case of a common malfunction. The manuals are also useful, or required, to understand the function of the various controls, whether hardware or software, when they need to be used, changed, or reset.

Reference manuals are generally used by maintenance personnel or by programmers, i.e., by people whose time is very expensive. The unavailability of reference manuals in a time of crisis can be very costly.

In addition to the usual documentation, it is a good precaution to summarize the main settings and operating recommendations for all commonly used hardware and software modules, and to post them or include them in a basic *installation manual.* Don't hesitate to draw the normal position of each switch for each device that may be tampered with by maintenance personnel or by an untrained or malicious user. Also, list and summarize all the main commands available with each specific program.

Manuals should be kept in an obvious place, and they should be readily available to the user. Manuals should never be removed from the computer room.

SOFTWARE DOCUMENTATION

The recommendations presented above for hardware documentation also apply for software documentation. We will now present additional recommendations that apply for software.

Software manuals are frequently consulted. They should be kept in duplicate. One set of software manuals should be kept at the installation site and another set should be available for consultation off-site. Whenever possible, software manuals should be supplemented with instructional notes, reference books and summaries of the most frequently used commands or instructions.

Unfortunately, most software manuals are so poorly written and hard to understand that many operators are hesitant to use them. It is therefore important to train each new operator in the use of both the hardware *and* the software resources of the system. A few computer operators or users will be capable of understanding and using the information presented in the manuals without help, but many will not. It is also useful to indicate the name and telephone number of a person who can provide additional information on, or help with, the software being used, for times when problems develop.

It is also generally useful to provide a comprehensive list of all software

available on your installation, even though all *original* copies of the software are kept at a remote site, rather than in the computer room itself. This will avoid unnecessary frustration, duplicate purchases of utility programs, and the retyping or redeveloping of existing data or programs.

RECORD OF CHANGES

All changes and modifications should be recorded in the computer log book and all hardware tinkerers, programmers, installers, and operators should be instructed to use the log book properly. All malfunctions should be recorded along with the circumstances at the time that they occur. Without such a log, proper diagnostics may be difficult or even impossible. Also unrecorded changes will often result in unexplained failures of older versions of programs or files.

SUMMARY

The need for documentation has already been explained in previous chapters. In this chapter we have stressed that the availability of proper documentation is essential for system operation.

Whenever a single reference manual is missing, there is a chance that a malfunction will occur that cannot be remedied without obtaining specific information from that missing manual. A highly competent person coming to remedy a malfunction will not be able to proceed without the required reference manual. This will result in much wasted time, wasted temper, a high cost and the possibility that the problem will not be remedied quickly. Such frustration should always be avoided by keeping complete and up-to-date documentation available on-site.

User manuals are equally important to the effective use of your computer system, and you may have to prepare your own operating instructions and summaries if a system is going to be used by several persons.

In short, don't neglect documentation.

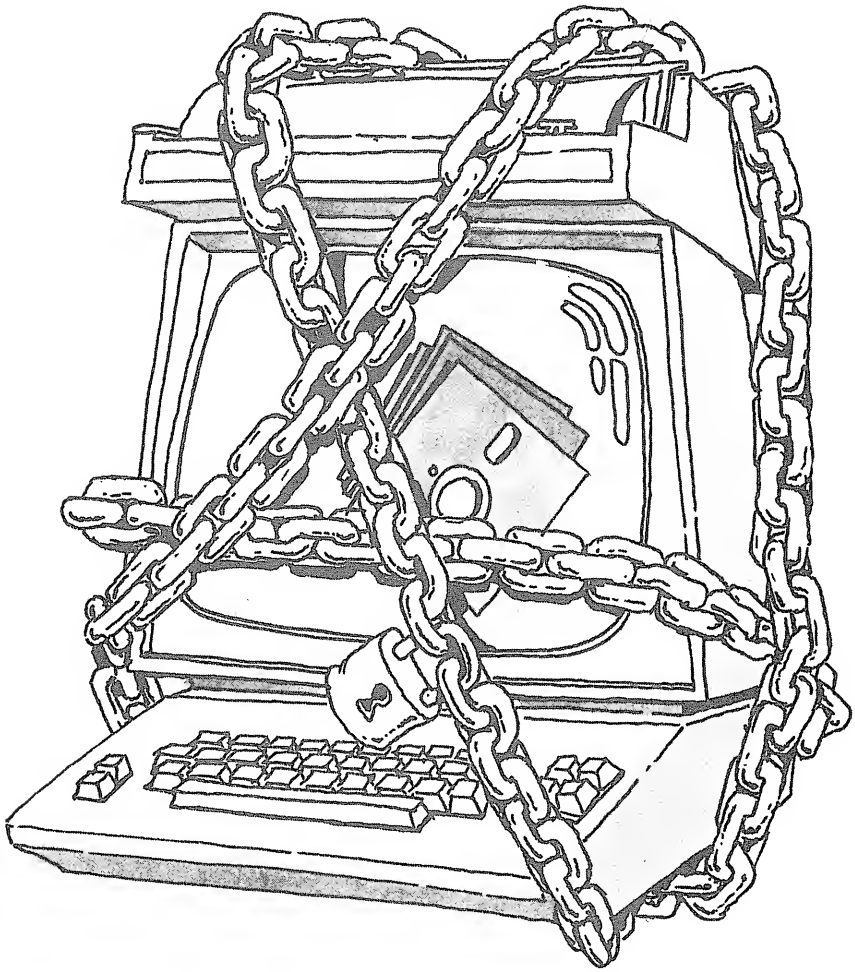
CHAPTER 12
SECURITY

Once harm has been done, even a fool understands it.
— *Homer,* The Iliad i.b. XVII, 32

INTRODUCTION

Securing information within and around a computer system can be accomplished by various means: psychological, legal, physical, organizational, and computerized (i.e., programmed). Some common methods will be reviewed here.

Programs and data must be secured against accidental damage and unauthorized access or copying. Preventing damage to a program or to data can be accomplished by following proper procedures. In particular, it can be accomplished by backing-up every new program received and



by creating backup copies of new data. Physical protection of storage media such as disks and tapes is accomplished by storing them in an appropriate manner, as explained in previous chapters. Securing programs and data against unauthorized access is a more difficult task, but it can be achieved. In most cases, it can be done by erecting a variety of barriers.

ERECTING BARRIERS

Confidential files can be marked as such with a special label and should be stored at a secure or remote location. Common sense should be used in preventing access to such locations by unauthorized personnel. In particular, computer operators may require constant access to a disk file cabinet in order to use various business programs. Confidential business files should not be stored in the same file cabinet, but in a separate locked one. Don't mix restricted access files with general access programs.

As another simple barrier, do not make blank magnetic material such as diskettes or tapes readily available. A user wishing to make a copy of a confidential file will require a magnetic medium such as a diskette or tape to make the copy. Leaving blank diskettes or tapes lying around the computer room is an open invitation to making easy copies.

At the psychological level, the fact that you intend to enforce the confidentiality of sensitive business files can be advertised by several methods. One method consists of labeling such disks or tapes as confidential and storing them in a separate location. In addition, all persons having access to the computer room or to a computer terminal can be required to sign appropriate confidentiality agreements stating that they will not obtain, copy, or remove any confidential information from the system. This opens up a clear and non-ambiguous threat of legal prosecution. In addition, business files may be "seeded" by inserting special markers at inconspicuous locations within the file. For example, a fake name or address may be entered in a list. Then, if an illegal copy is made, this unique name and address will serve as proof of the theft.

Naturally, listings containing confidential business information should not be left lying around the computer room but should be disposed of properly. Preferably, they should be shredded. Larger computer installations often provide special secure waste baskets in the computer room that only allow the insertion of paper listings, and can only be emptied with a key. The contents are then shredded by authorized personnel.

Also be aware that the availability of a computer system and a printer encourages the proliferation of business printing. Many printouts contain sensitive business information, yet the proliferation is such that it is impossible to destroy them all manually. In such cases, a shredding machine

should be used. A good shredder is relatively expensive, but indispensable to maintain confidentiality of business information. Finally, it is best to locate the computer room so that access to and from the room can be monitored by office personnel who are close by.

PROTECTING FORMS

Special forms are available to protect you from forgeries and unauthorized duplications. In particular, special inks may be used that will cause part of a form to be either invisible to a copier, or to become visible only on the copy. The first technique is called a *dropout*; the second is called the *hidden word*. In the latter case, the background is generally imprinted with a design that appears random or geometrical. When a copy is made, a word such as "UNAUTHORIZED" or "VOID" stands out on the copy.

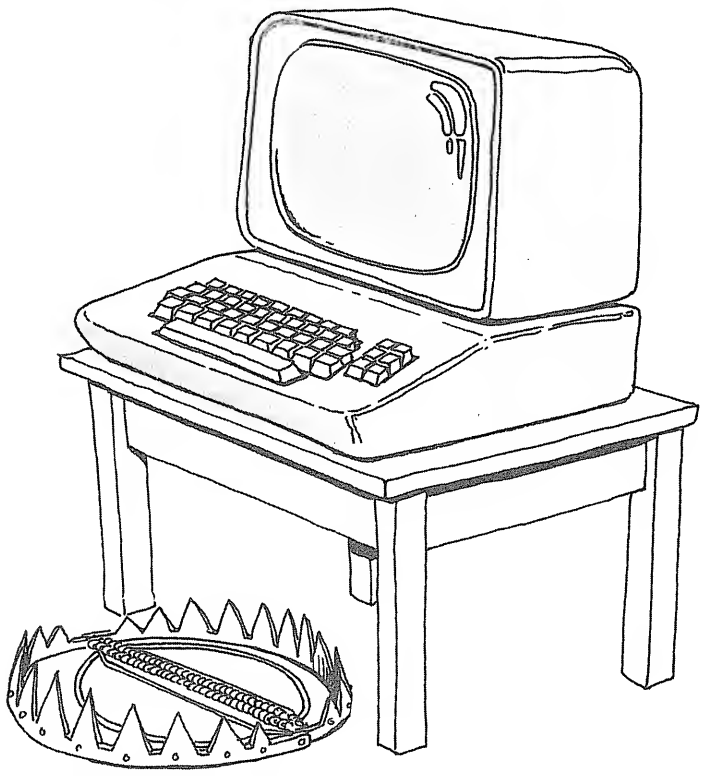
Similarly, pantographs may be used that include combinations of screened colors and densities, which result in uneven copies, that look like obvious duplicates.

When printing checks, you may guard against alterations by using a high impact force on the printer in order to punch partially through the paper, or by using a background color or design that is erased by any attempt at forgery, or even by using safety stains.

SECURING THE SITE

When site security is required, one of the simplest and most effective methods is to keep everything under lock and key. Access to the computer room can be controlled and, if necessary, all accesses can be entered into a log. As an additional precaution, the computer proper can be equipped with a lock and key. Similarly, the ON/OFF switch on most CRT terminals can be replaced with a key lock. It is also a good precaution to keep all essential programs and data in locked cabinets.

Naturally, these drastic measures will severely limit the number of authorized users, and may discourage the use of the computer. In view of the inconvenience of such an approach, alternative, softer protection techniques may be used. In particular, a number of operating systems and access control programs have been designed to provide a password access to protect the programs and files. An authorized user must then type the proper password in order to either read a specific file or execute a given program. Passwords must be changed frequently in order for the system to retain its effectiveness.



When additional security is required, it is possible to use a program that records the time at which the computer is being used and the (alleged) name of the user.

Sophisticated operating systems and file management programs also allow users to protect their files selectively by making them read-only, executable-only, or even totally inaccessible except to the owner of the file. These features cannot be added by the user. They are part of the file system, i.e., generally part of the operating system.

ENCRYPTION

Whenever additional security is necessary to protect the contents of files from unauthorized reading, a simple method for protecting files is to encrypt data files. This makes them unreadable to a user without the proper deciphering code or program. A cipher program will take a given file and convert sequences of characters in the file into another sequence of characters according to some encryption algorithm. The resulting

material is totally unreadable to a human and will seem completely meaningless to another user. Using an appropriate decryption program, it can be converted back to its original form.

The disadvantage to this approach is the time required to encrypt and decrypt files. However, it is a very effective tool as it discourages copying information that is not readily identifiable. Naturally, the label on the disk or tape should not explicitly state its contents, or the purpose of the encryption algorithm will be partially defeated, since the nature of its contents will be revealed.

AUDIT TRAILS

There is a more subtle type of security breach which has to do with breaching the procedures themselves rather than obtaining illegal access to the computer. For example, a dishonest employee may obtain access to the check printing program and print illegal checks to his or her name and then later apply fictitious credit, or write up a non-existing sale or return to make up for the missing money. In order to prevent such occurrences, audit trails must be available for all financial records. Briefly stated, this means that any change to files in the system must be documented so that it is possible to correlate all successive changes in the files. In particular, a summary of all transactions should be printed before changes or transactions are entered into permanent files. Such audit trail printouts should be collected daily and stored in a secure, remote place so that no one can modify them. They should become part of the permanent records of the financial system.

COMPUTER THEFT

Throughout this book we have presented the rules and proper procedures which, when applied consistently, will result in reliable computer operation. Most of the recommendations were aimed at preventing *involuntary* harm to the system or the operator. Unfortunately, computer security involves more than involuntary actions; it also encompasses theft and crime. For completeness, we will now review a list of common abuses, describe a set of countermeasures, and examine the special problems inherent to computerized record handling.

The Abuses

Abuses with computers bear the same names as those listed in the civil and criminal codes: theft, embezzlement, larceny, sabotage, invasion of

privacy, break-in, espionage and extortion. Abuses fall in three main categories:

- securing funds in an unauthorized manner
- securing information in an unauthorized manner, with an intent to use it for financial gain or to some other advantage
- willful destruction of information or harm to the system as an act of malice, unfair business, or revenge.

Unfortunately, these abuses are much harder to detect, in the case of a computer, than they are under other circumstances. This is due both to the nature of computer systems, where all information is encoded in a complex format, and to the attitude of many business managers who do not completely understand how their computer system operates.

These issues should be considered seriously, before they become a liability. Whenever a computer is used for business purposes and valuable information is entrusted to it, it is essential that potential security risks be examined carefully. Let us now look at common countermeasures. Countermeasures fall in two broad categories: technical and operational.

Technical Countermeasures

Many of the technical countermeasures have already been presented in this chapter. They include high quality *access control programs* that automate and control access to programs as well as to data files. Typically these access control programs use passwords and other codes, and restrict specific users to authorized files and programs only. They can also automatically record and report accesses to the system or to sensitive files in the system. In addition sophisticated control programs will only authorize *specific functions* by *specific classes* of users. In particular, the type of access to each file, as well as the list of authorized persons, may be automated.

Encryption and *scrambling* of information may be used to protect files, both when they are stored on a magnetic medium and when they are transmitted over telephone lines.

Operational Countermeasures

Operational countermeasures are even more important than the technical ones. These countermeasures fall in three categories: asset protection, risk analysis and organizational safeguards.

Asset Protection

From a security standpoint all business assets should be systematically protected. This includes the computer equipment, all other equipment, the building proper, and all business records, whether in printed or magnetic form. Protecting assets involves both preventive measures as well as back-up solutions in case harm does occur. Clearly, preventive measures that will prevent harm from occurring are more important. Preventive techniques include a systematic access control as well as comprehensive protection techniques, including environmental, electrical and fire.

Proper computer access control procedures should be used that apply to all personnel, and in particular to personnel accessing valuable business files. Computer access should be restricted to designated terminals, and the permitted types of actions on each terminal, such as order entry, financial reports or inventory updates, should be clearly known.

Ideally, each terminal should have a well-defined function. For example, a terminal used for sales data reporting or for marketing purposes should not be usable for accessing or modifying financial data. Similarly a terminal used to update the inventory should not be usable for performing changes in the customer data base or in the sales file. Special access control programs are usually responsible for restricting the role of each terminal. However, whenever these methods cannot be used, other barriers should be erected. Such barriers may include key locks on the terminals themselves as well as physical separation of data whenever possible. For example, financial data may be stored on a separate file, recorded on a separate medium, and kept in the physical possession of a suitable person. This file should not reside on the main system disk while unrelated tasks are being performed.

Always think defensively. If all your data files are available on a single support, such as a disk, on line, they may be accessed by unauthorized users. Even if you are using a sophisticated access control program, an unauthorized person might simply duplicate the entire disk, then work on it at leisure to extract the information wanted. Similarly, the handling of media should be carefully restricted. Do not offer unauthorized personnel the opportunity to damage, contaminate, or copy your magnetic records. And finally, careful backup procedures should be used in the event a mishap does occur.

Risk Analysis

Because of the large variety of computer systems and software in use in business, each installation imposes different limitations and requirements

that evolve in time. It is important to regularly conduct an evaluation of the risks posed by the specific methods you are using. Always try to think of the ways your security measures can be defeated. Most importantly, have all systems and data audited at suitable intervals by a qualified person. Unfortunately, many professional auditors such as certified public accountants are unfamiliar with the internal operation of computer systems and are therefore not capable of making the proper recommendations. Be aware of this limitation when selecting the person or organization that will perform the audit.

Organizational Safeguards

One of the great risks in computer installation is the *blind trust* approach. In many cases, managers or consultants do not understand enough about the internal operation of the computer system and rely on one person within the organization. This may happen at many levels. The Chief Executive Officer might rely on the Chief Financial Officer. The Chief Financial officer might rely on the Head of Computer Operations. This goes on all the way to the computer input operator and the maintenance person in charge of hardware or software, or even to the building maintenance or janitorial service. Be aware that any one of these persons, if they know what they are doing, has the capability to perform unauthorized actions. Systematic controls should be used to check for these possibilities.

Unfortunately, many companies that previously used strict control procedures when they used manual accounting systems, now seem to rely blindly on computer statements since they have switched to a computer system. Do not relax your vigilance. Continue to perform systematic checks of all the data at frequent intervals. In particular, continue to follow the normal audit guidelines. Regularly check the payroll to insure that amounts are not inflated or fictitious. Check the accounts payable file to verify that suppliers exist and that goods or services have been delivered. Reconcile cash with the statements. Reconcile the physical inventory with the inventory listed by the computer program.

It is important to run a number of manual checks and cross verifications on all output from a computerized system. In the case of large companies, special audit programs have been developed that perform many of these checks automatically. In particular, such programs will automatically flag any person receiving an unusually large amount of overtime pay, and they will list the names of new employees, as well as the names of employees receiving a larger amount of money in any one month. They will also flag

unusual expenditures and other statistical deviations. There is, however, no substitute for frequent, common sense verifications. Unfortunately, computer crime is often characterized by the fact that an unauthorized action is performed only once, with dire consequences that do not show up until later. Unless checks are frequent and consistent, the loss may not come to light until it is too late.

As an important procedural protection, just as in the case of a manual system, *separation of duties* should be enforced. No one person should handle a complete transaction from beginning to end. In particular, the following should be carefully separated: recordkeeping, transactions on any assets, decision-making, and physical keeping of the assets. As an example, and at a minimum, the person opening the mail or receiving the payments must be different from the person doing the bookkeeping, who must be different from the person in charge of reconciliation, who must be different from the person in charge of controlling or auditing the operation. In particular, the person doing the programming must always be different from the person in charge of operating the system, i.e., in charge of the data entry and other transactions on the system. Let us now examine the specific dangers presented by a dishonest programmer.

Programmer Fraud

Many special problems are inherent to computer systems. They include poor audit trails, the inability of upper management and auditors to fully understand the way information is handled, the concentration of valuable information in a small amount of storage space, and, finally, the unique role of the programmer who designed the system being used. We have already described most of these problems. Let us now consider the role of the programmer.

The programmer who designed the computer system is one of the major potential security risks to that system. The reason is that practically no one besides the programmer will ever fully understand all of the features in the program being used. As a result, the programmer must be honest and trustworthy or he or she has the capability to perform a number of unauthorized or criminal acts while escaping easy detection.

Acts stemming from programmer fraud have been given descriptive names such as logic bombs, trapdoors, trojan horses and salamis. Let's examine them.

A *logic bomb* is analogous to the time bomb we have described in this book, except that it is quite deliberate. A logic bomb is a special program that will be activated sometime in the future once the programmer has left.

The intent may be malicious, mischievous, or dishonest. For example, a programmer may write the programs in such a way that the whole system will grind to a halt once a specific number is reached. This number could be the value of a transaction, or it could be a date. Similarly, a programmer could conceivably set up a future transfer of funds to a secret bank account and escape detection for a long enough period of time for him to have the money removed from that account and and leave no traces. When an entire system has been designed by just one person or even by a small number of persons, there is little protection against such actions, except systematic monitoring and auditing.

Trapdoors are possibilities for unauthorized or unanticipated actions that were left in the program by accident rather than by design. Because a program can never be guaranteed error-free, there may be accidental errors that allow an unauthorized user to access the system and perform unauthorized actions. This has been especially true in the case of larger systems connected in a network or using telecommunication lines. In this case, remote users (in one instance, school children no older than twelve) have been able to break into large data bases and perform a number of unauthorized actions, ranging from the modification of school grades to access of high-security company and government files. Again, proper monitoring, access control and auditing will limit such risks.

A *trojan horse* is a deliberate addition of features to a program that will permit a later access by the programmer in a way that will not be recorded by the rest of the programs. This may include program facilities that defeat all known features of the access control programs, or special preprogrammed commands that allow or facilitate tampering with files and breaking into various parts of the system. Clearly, a trojan horse is one of the most difficult problems to detect.

Salamis are techniques that will slice away at portions of large transactions in virtually undetectable ways. Thus, thin slices of information or money can be transferred to the dishonest programmer's account. For example, in a company purchasing large quantities of a given item, the internal price computation could be rounded up or down to the nearest cent. The money thus "lost" by the rounding-off process can then be diverted to a personal account. Provided such transactions affect large numbers of items, the resulting sums could be very sizable over a period of time. Small amounts of money can be "lost" with no immediate consequences since the discrepancies can be qualified as minor on a day-to-day basis.

As a result of these special risks, the basic recommendation is to deny programmers all access to their software once it is being used on a computer. In addition, they should be denied any access whatsoever to any

business files. Unfortunately, this restriction is hard to enforce in small organizations where the external programmer or the in-house computer genius is on friendly terms with everyone. If you decide to break this rule, be aware of its potential consequences.

A SUMMARY OF SECURITY PROCEDURES

Do not underestimate the psychological element for safeguarding a system. In a small system, whenever possible, one person should be held responsible for the integrity of the programs and data within the installation, and should be encouraged to demonstrate this concern in a visible manner. In any environment, if it is known that one person is responsible for security and for enforcing the integrity of the computer system, breaches are less likely to occur, almost regardless of the specific measures taken.

Many security procedures can be used. Each one, by itself, has only limited effectiveness, but, when used together, they present a suitable obstacle to accidental or planned interference with the system's security.

CHAPTER 13
HELP

The spirits that I summoned up I now can't rid myself of.
— *Goethe,* The Sorcerer's Apprentice

INTRODUCTION

Proper procedures and preventive maintenance will prevent most failures and will insure reliable, continuous operation. In this chapter, we will review the two types of maintenance required, examine how to secure maintenance services, and present the recommended procedures when the system fails.

THE TWO TYPES OF MAINTENANCE

Two types of maintenance must be performed on a computer system: *preventive* maintenance and *remedial* maintenance. Preventive maintenance aims at avoiding and preventing malfunctions. Remedial maintenance aims at correcting malfunctions after they have occurred. Specific maintenance recommendations have been presented for each device in the preceding chapters. We will summarize here the overall approach.

Most preventive maintenance is accomplished by the user or operator. However, some types of specialized preventive maintenance should only be performed by qualified personnel. Such maintenance includes, for example, printer maintenance, where a specialist comes once every three or six months, and disk maintenance, where the alignment is checked every six or twelve months.

In order to facilitate diagnostics and maintenance, some vendors provide diagnostic programs that can be used to test each piece of equipment at regular intervals. These programs should be run at the recommended intervals to verify that all system elements are operational.

Remedial maintenance is usually performed by one or more specialists. We will now examine how to secure such maintenance services.

SECURING MAINTENANCE SERVICES

If your system is used at home, and it is in need of repair, it is usually acceptable to bring part of the system to a store or service center and wait several days for the repair. However, if your system is used for business, no part of the system may be removed, and immediate service is usually necessary or business paralysis may occur. Unless you have the in-house capability to maintain and repair your system, you should secure appropriate maintenance services before a malfunction occurs.

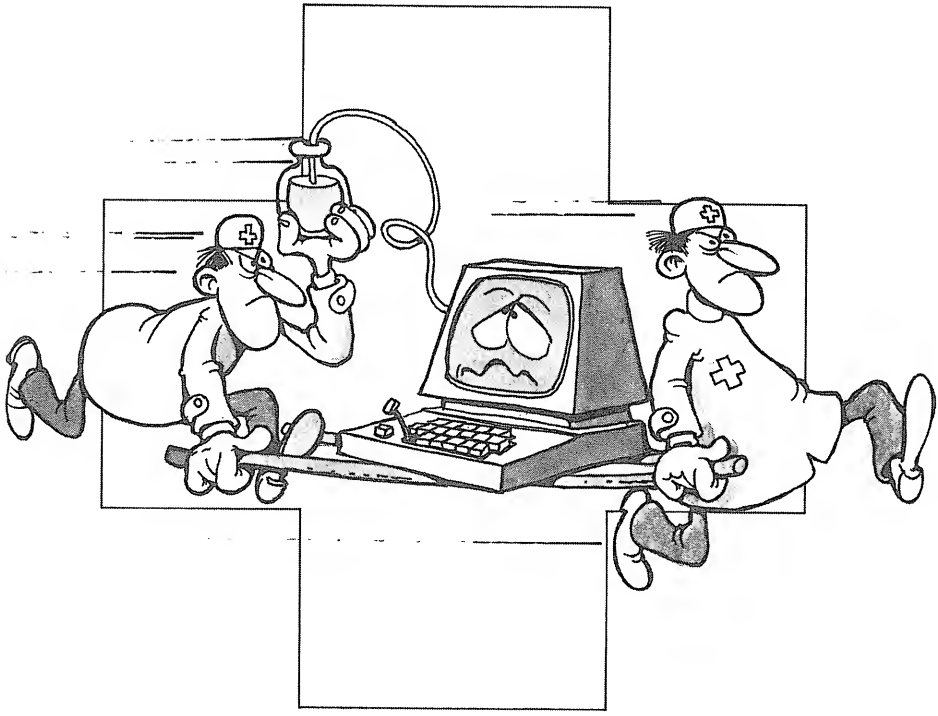
You can obtain two types of maintenance services: comprehensive maintenance of the complete system by one vendor, or piecemeal maintenance of each item in the system. The first solution is by far the best. Whenever a malfunction occurs, it is often difficult to determine which

element of the system is causing the malfunction. When different vendors are providing maintenance for various elements of the system, it is sometimes a hopeless proposition to determine which device is at fault, since each maintenance person will readily assume that the problem does not lie with the equipment that he or she is responsible for.

The general guideline when estimating maintenance cost is 1% of the system cost per month for maintenance services.

Many specialized companies provide maintenance services for specific printers, CRT terminals, and other common peripherals. However, let us stress again that, whenever possible you should try to obtain maintenance services for the complete system. Ideally, this should include maintenance for both hardware and software since it may at times be difficult to determine whether the hardware or the software is at fault. Unfortunately, in many cases, the best that one can hope for is to secure separate hardware and software maintenance.

Here is a brief guide to self-help to use when your system fails.



WHEN IT DOESN'T WORK

In any casual environment when the system fails, almost regardless of the incident, you can reasonably suspect the human operator first, then the software, and then the hardware. Naturally, with a trained operator, the order should be reversed. What this means in practice is the following. When a malfunction occurs, assume first that you or another user has made some mistake. Try again the sequence of operations that led to the problem. If the problem occurs again, shut down the entire system and restart everything. Odds are that the problem will be cleared up. This will usually indicate that there has been an operator error. An incorrect command may have been used, or an improper sequence may have been utilized. However, a malfunction may sometimes be due to electrical noise, as well as faulty hardware or software.

If the above procedure doesn't solve the problem, suspect the software copy you are using, i.e., the disk or tape. Make a clean copy of your programs using a fresh disk or diskette, and try again. If the problem disappears, this indicates that the copy of the software you were using had been contaminated either by dust or by operator mishandling. If a faulty diskette was the problem, dispose of it. If a faulty disk was the problem, mark it appropriately so that it will not be used by another operator in its present condition.

If you have followed these steps and the problem still doesn't clear up, or comes back repeatedly, suspect the hardware (including the environment). Check all of the mechanical connections, starting with the obvious ones. Check all cables. Make sure that the proper cables are used and that they are properly plugged in or attached with secure connections. Make sure that there are no loose or bent pins outside or inside the boxes of equipment. Make sure that the power cords are properly connected and that all fuses are intact.

If this approach fails, and you are unable to determine which piece of equipment is at fault, turn the system off and check the proper contact of each printed circuit board. If you can determine that a specific printed circuit board is at fault, verify that all chips are properly inserted. You may have to remove the board and perhaps some components in order to clean all the contacts if they are visibly corroded. In many cases, the cleaning will solve the problem.

If the problem persists—and in particular if it is occurring erratically—it may be caused by too high a temperature. To reduce the temperature of a given device, begin by turning on your air conditioner. If you don't have one, or if the case is extreme, remove the cover of the device and use a fan.

When attempting to diagnose a problem, the essential axiom is: divide and conquer. The main difficulty lies in isolating the system component that is at fault. If you are fortunate enough to detect an obvious malfunction, such as a misbehaving printer or a misbehaving disk drive, then follow the trouble-shooting recommendations presented in the corresponding peripheral manual.

Whenever you cannot determine which module or component is at fault, start systematically exchanging each module with another (good) one. For example, exchange the printer, the CRT, and the computer. Within a device, exchange the boards. If the module used to replace another one makes the system work, then this indicates the logical component that was at fault. When successful, this method allows you to isolate the cause of a problem simply.

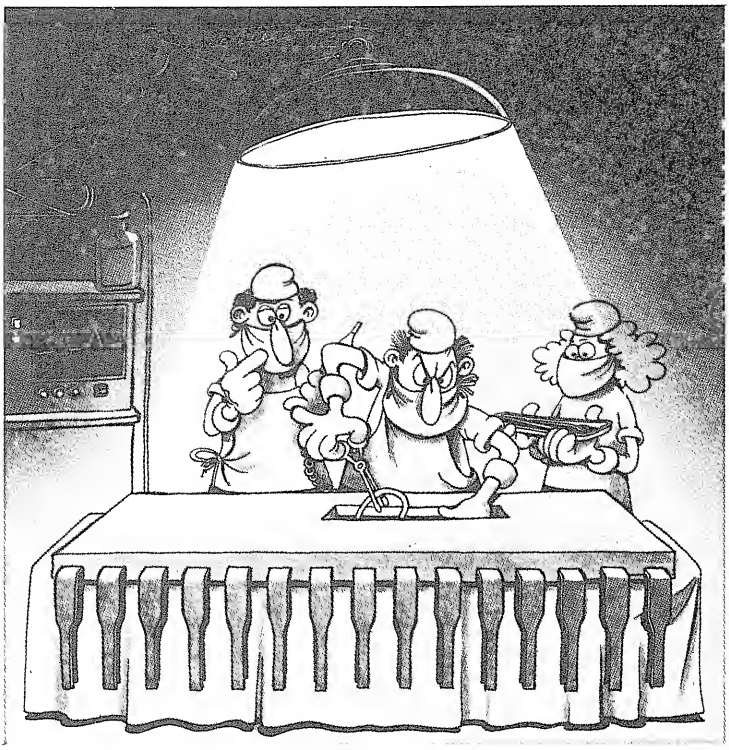
With experience, you will become attuned to most of the common failure modes of a system, and you will probably be in a position to remedy all *common* malfunctions on your system.

If you are responsible for maintaining your system, it is suggested that you be present every time that an outside maintenance person comes to correct a malfunction. You may be able to learn the proper procedures to follow, or discover how to remedy the situation if it happens again. And, more importantly, you might learn how you can prevent the problem from happening again. You will usually discover that most malfunctions are caused by operator mishandling or lack of respect for the proper operating instructions.

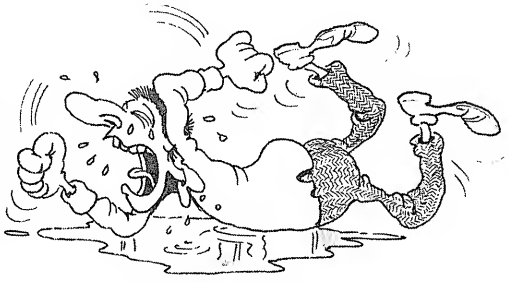
Naturally, in some cases, you will discover that the malfunction is due to a faulty program or to faulty hardware. This type of malfunction is usually not caused by the operator. However, this is not always the case. For example, an overanxious operator may operate the system at a higher temperature for a long period of time, thereby enhancing the probability of chip failure in a shorter amount of time. This will later be diagnosed as a hardware problem even though it was originally caused by a negligent operator.

If you are in doubt at any point about what to do, or if you do not feel competent to pursue the diagnostics, then stop. Don't attempt to go on. It is now time to call in the appropriate maintenance person.

Don't ever open the equipment and probe around inside unless you know exactly what you are doing. If you have this competence, then first turn off all of the equipment and strictly follow the procedures recommended by the manufacturer. But remember: while probing inside the electronic equipment, you may cause harm to yourself as well as to the equipment. In addition to receiving an electrical shock, you might inad-



vertently short pin connections and damage circuits without realizing it. Here is a horror story.



With some home computer systems, it is the user's responsibility to insert additional memory chips in order to expand the memory. Sometimes, memory chips are exchanged in order to install a different monitor program. In this case, the user first removed a memory chip and then reinserted it. Unfortunately, during the process, one of the pins broke. Since the user did not have a spare memory chip available, he found an ingenious way to correct the problem, by

inserting a pin in the socket. This did correct the problem. However, a few days later, the computer began behaving erratically. The problem was not immediately diagnosed and when the system was opened up, everything seemed to be in order. Eventually, blue smoke began rising from the system, and then suddenly it died. The culprit was discovered when the damaged memory chip was found and a loose pin was discovered in the enclosure. The pin had become dislodged from the socket and fallen out.

As the pin became dislodged, the corresponding memory chip stopped operating reliably which resulted in the erratic system behavior. Then, the pin fell out, eventually shorting two connections and burning out several integrated circuits in one board, thus requiring an expensive repair. Again, don't do it unless you know exactly what you are doing.

SUMMARY

Your computer system is very reliable and will probably not fail as long as you follow the proper procedures. In a business environment, however, you must anticipate the possibility of a failure and secure maintenance services, preferably from a single vendor, before they are actually necessary.

Should a failure occur, perform as many simple checks as possible by yourself. You will be able to remedy common problems such as loose cables and contaminated diskettes by following the recommendations we have presented in this book. In many cases, you may never require any maintenance except preventive maintenance visits for disk drives and printers.

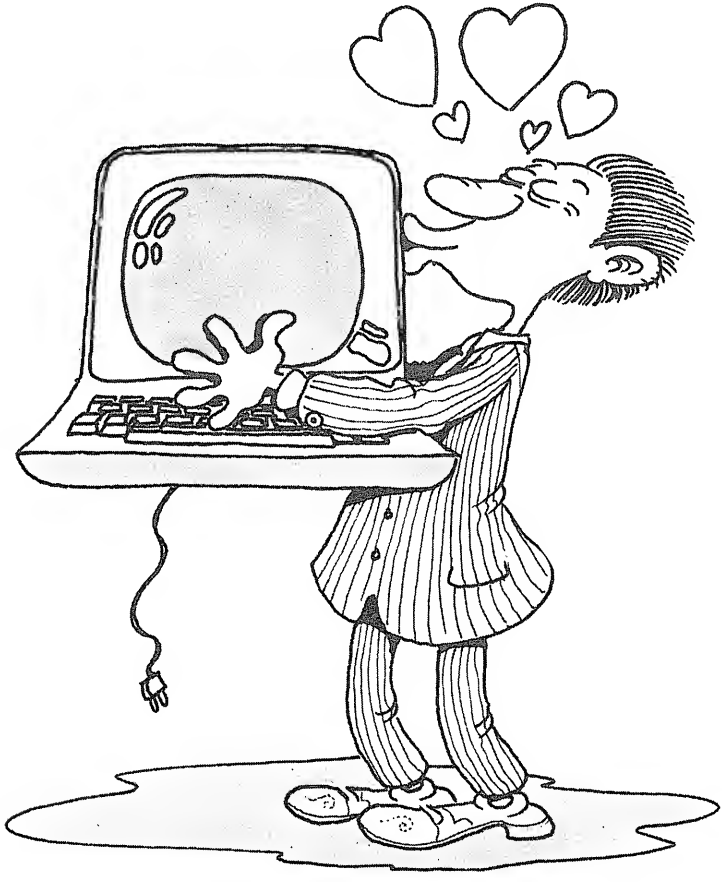
CONCLUSION

Computer systems and their peripherals have become highly reliable. Provided you use well-designed, well-tested and well-documented hardware and software, you will achieve highly reliable and effective use of your computer by following a number of simple recommendations. The purpose of this book was to teach you the proper procedures, alert you to possible difficulties, and present you with effective solutions. The author hopes that this goal has been achieved.

In many cases, you will find that you need to use only a small subset of all the recommendations that are presented here. This is because the sources of potential problems are many, and while all should be known to the serious computer user, only a few will apply in each case. A major goal of

this book, therefore, is to make you aware of all important potential problems.

Hopefully, on each computer installation, only a few of these procedures will need to be enforced each time a new user accesses the system. Don't forget that the system is as vulnerable as its weakest link, and the weakest link is usually the human user. Hopefully, after reading this book, the only limitation to the reliability of your system will be its hardware and software. The author will be pleased to receive comments from interested readers—including horror stories!



APPENDIX A
TAPE AND DISKETTE MANUFACTURERS

3M (Scotch)
AMPEX
ATHANA
BASF
CONTROL DATA
DYSAN
GRAHAM
IBM
MAXELL
MEMOREX
NASHUA
NATIONAL CO
SHUGART
SYNCOM
VERBATIM
WABASH

APPENDIX B
USEFUL ADDRESSES

American Society for Industrial Security (ASIS)
2000 K Street, NW, Suite 651
Washington, DC 20006

Committee on National Security Companies (CONSCO)
161 William Street
New York, NY 10038

Computer Security Institute
5 Kane Industrial Drive
Hudson, MA 01749

EDP Security
181 West St.
Waltham, MA 02154

National Fire Protection Association (NFPA)
470 Atlantic Avenue
Boston, MA 02210

Security Equipment Industry Association (SEIA)
Santa Monica, CA 90405

National Bureau of Standards
Washington, DC 20234

Underwriters Laboratories
333 Pfingsten Road
Northbrook, IL 60062

References

- National Fire Protection Association (NFPA), 60 Batterymarch Street, Boston, MA 02110:

  NFPA 10: Installation of Portable Fire Extinguishers

  NFPA 10A: Recommended Good Practice for The Maintenance and Use of Portable Fire Extinguishers

  NFPA 46A: Floor Covering

  NFPA 70: National Electrical Code

  NFPA 75: Protection of Electronic Computer/Data Processing Equipment

  NFPA 78: Lightning Protection Code

  NFPA 90A: Installation of Air Conditioning and Ventilation Systems (non-residential).

  Fire Journal

- American Society of Heating, Refrigeration and Air-Conditioning Engineers:

  ASHRAE Handbook

- National Board of Fire Underwriters:

  NBFU 70

- Underwriters' Laboratories, Inc.:

  U.L. Handbook 478

Index

The SYBEX Library

BASIC PROGRAMS FOR SCIENTISTS AND ENGINEERS

by Alan R. Miller 340 pp., 120 illustr., Ref. B240

This second book in the "Programs for Scientists and Engineers" series provides a library of problem solving programs while developing proficiency in BASIC.

INSIDE BASIC GAMES

by Richard Mateosian 350 pp., 240 Illustr., Ref. B245

Teaches interactive BASIC programming through games. Games are written in Microsoft BASIC and can run on the TRS-80, APPLE II and PET/CBM.

FIFTY BASIC EXERCISES

by J.P. Lamoitier 240 pp., 195 Illustr., Ref. B250

Teaches BASIC by actual practice using graduated exercises drawn from everyday applications. All programs written in Microsoft BASIC.

EXECUTIVE PLANNING WITH BASIC

by X.T. Bui 192 pp., 19 illustr., Ref. B380

An important collection of business management decision models in BASIC, including Inventory Management (EOQ), Critical Path Analysis and PERT, Financial Ratio Analysis, Portfolio Management, and much more.

BASIC FOR BUSINESS

by Douglas Hergert 250 pp., 15 illustr., Ref. B390

A logically organized, no-nonsense introduction to BASIC programming for business applications. Includes many fully explained accounting programs, and shows you how to write them.

BASIC EXERCISES FOR THE APPLE

by J.P. Lamoitier 230 pp., 80 illustr., Ref. B500

For all Apple users, this learn-by-doing book is written in APPLESOFT II BASIC. Exercises have been chosen for their educational value and application to math, physics, games, business, accounting, and statistics.

YOUR FIRST COMPUTER

by Rodnay Zaks 260 pp., 150 Illustr., Ref. C200A

The most popular introduction to small computers and their peripherals: what they do and how to buy one.

DON'T (or How to Care for Your Computer)

by Rodnay Zaks 220 pp., 100 Illustr., Ref. C400

The correct way to handle and care for all elements of a computer system including what to do when something doesn't work.

INTRODUCTION TO WORD PROCESSING

by Hal Glatzer 200 pp., 70 illustr., Ref. W101

Explains in plain language what a word processor can do, how it improves productivity, how to use a word processor and how to buy one wisely.

INTRODUCTION TO WORDSTAR

by Arthur Naiman 200 pp., 30 illustr., Ref. W105

Makes it easy to learn how to use WordStar, a powerful word processing program for personal computers.

FROM CHIPS TO SYSTEMS: AN INTRODUCTION TO MICROPROCESSORS

by Rodnay Zaks 560 pp., 255 illustr., Ref. C201A

A simple and comprehensive introduction to microprocessors from both a hardware and software standpoint: what they are, how they operate, how to assemble them into a complete system.

MICROPROCESSOR INTERFACING TECHNIQUES

by Rodnay Zaks and Austin Lesea 460 pp., 400 Illustr., Ref. C207

Complete hardware and software interconnect techniques including D to A conversion, peripherals, standard buses and troubleshooting.

PROGRAMMING THE 6502

by Rodnay Zaks 390 pp., 160 Illustr., Ref. C202

Assembly language programming for the 6502, from basic concepts to advanced data structures.

6502 APPLICATIONS BOOK

by Rodnay Zaks 280 pp., 205 Illustr., Ref. D302

Real life application techniques: the input/output book for the 6502.

ADVANCED 6502 PROGRAMMING

by Rodnay Zaks 300 pp., 140 Illustr., Ref. G402A

Third in the 6502 series. Teaches more advanced programming techniques, using games as a framework for learning.

PROGRAMMING THE Z80

by Rodnay Zaks 620 pp., 200 Illustr., Ref. C280

A complete course in programming the Z80 microprocessor and a thorough introduction to assembly language.

PROGRAMMING THE Z8000

by Richard Mateosian 300 pp., 125 Illustr., Ref. C281

How to program the Z8000 16-bit microprocessor. Includes a description of the architecture and function of the Z8000 and its family of support chips.

THE CP/M HANDBOOK (with MP/M)

by Rodnay Zaks 330 pp., 100 Illustr., Ref. C300

An indispensable reference and guide to CP/M—the most widely used operating system for small computers.

INTRODUCTION TO PASCAL (Including UCSD PASCAL)

by Rodnay Zaks 420 pp., 130 Illustr., Ref. P310

A step-by-step introduction for anyone wanting to learn the Pascal language. Describes UCSD and Standard Pascals. No technical background is assumed.

THE PASCAL HANDBOOK

by Jacques Tiberghien 490 pp., 350 Illustr., Ref. P320

A dictionary of the Pascal language, defining every reserved word, operator, procedure and function found in all major versions of Pascal.

PASCAL PROGRAMS FOR SCIENTISTS AND ENGINEERS
by Alan Miller 400 pp., 80 Illustr., Ref. P340
A comprehensive collection of frequently used algorithms for scientific and technical applications, programmed in Pascal. Includes such programs as curve-fitting, integrals and statistical techniques.

APPLE PASCAL GAMES
by Douglas Hergert and Joseph T. Kalash 380 pp., 40 illustr., Ref. P360
A collection of the most popular computer games in Pascal challenging the reader not only to play but to investigate how games are implemented on the computer.

INTRODUCTION TO THE UCSD p-SYSTEM
by Charles W. Grant and Jon Butah 320 pp., 110 illustr., Ref. P370
A simple, clear introduction to the UCSD Pascal Operating System for beginners through experienced programmers.

INTERNATIONAL MICROCOMPUTER DICTIONARY
140 pp., Ref. X2
All the definitions and acronyms of microcomputer jargon defined in a handy pocket-size edition. Includes translations of the most popular terms into ten languages.

MICROPROGRAMMED APL IMPLEMENTATION
by Rodnay Zaks 350 pp., Ref. Z10
An expert-level text presenting the complete conceptual analysis and design of an APL interpreter, and actual listings of the microcode.

SELF STUDY COURSES

Recorded live at seminars given by recognized professionals in the microprocessor field.

INTRODUCTORY SHORT COURSES:
Each includes two cassettes plus special coordinated workbook (2½ hours).

S10—INTRODUCTION TO PERSONAL AND BUSINESS COMPUTING
A comprehensive introduction to small computer systems for those planning to use or buy one, including peripherals and pitfalls.

S1—INTRODUCTION TO MICROPROCESSORS
How microprocessors work, including basic concepts, applications, advantages and disadvantages.

S2—PROGRAMMING MICROPROCESSORS
The companion to S1. How to program any standard microprocessor, and how it operates internally. Requires a basic understanding of microprocessors.

S3—DESIGNING A MICROPROCESSOR SYSTEM
Learn how to interconnect a complete system, wire by wire. Techniques discussed are applicable to all standard microprocessors.

INTRODUCTORY COMPREHENSIVE COURSES:

Each includes a 300-500 page seminar book and seven or eight C90 cassettes.

SB3—MICROPROCESSORS

This seminar teaches all aspects of microprocessors: from the operation of an MPU to the complete interconnect of a system. The basic hardware course (12 hours).

SB2—MICROPROCESSOR PROGRAMMING

The basic software course: step by step through all the important aspects of microcomputer programming (10 hours).

ADVANCED COURSES:

Each includes a 300-500 page workbook and three or four C90 cassettes.

SB3—SEVERE ENVIRONMENT/MILITARY MICROPROCESSOR SYSTEMS

Complete discussion of constraints, techniques and systems for severe environmental applications, including Hughes, Raytheon, Actron and other militarized systems (6 hours).

SB5—BIT-SLICE

Learn how to build a complete system with bit slices. Also examines innovative applications of bit slice techniques (6 hours).

SB6—INDUSTRIAL MICROPROCESSOR SYSTEMS

Seminar examines actual industrial hardware and software techniques, components, programs and cost (4½ hours).

SB7—MICROPROCESSOR INTERFACING

Explains how to assemble, interface and interconnect a system (6 hours).

SOFTWARE

BAS 65™ CROSS-ASSEMBLER IN BASIC

8" diskette, Ref. BAS 65

A complete assembler for the 6502, written in standard Microsoft BASIC under CP/M®.

8080 SIMULATORS

Turns any 6502 into an 8080. Two versions are available for APPLE II.

APPLE II cassette, Ref. S6580-APL(T)

APPLE II diskette, Ref. S6580-APL(D)

FOR A COMPLETE CATALOG OF OUR PUBLICATIONS

U.S.A.
2344 Sixth Street
Berkeley,
California 94710
Tel: (415) 848-8233
Telex: 336311

SYBEX-EUROPE
Centre Paris Daumesnil
4 Place Felix Eboué
75583 Paris Cedex 12
Tel: 1/347-30-20
Telex: 211801

SYBEX-VERLAG
Heyestr. 22
4000 Düsseldorf 12
Germany
Tel: (0211) 287066
Telex: 08 588 163

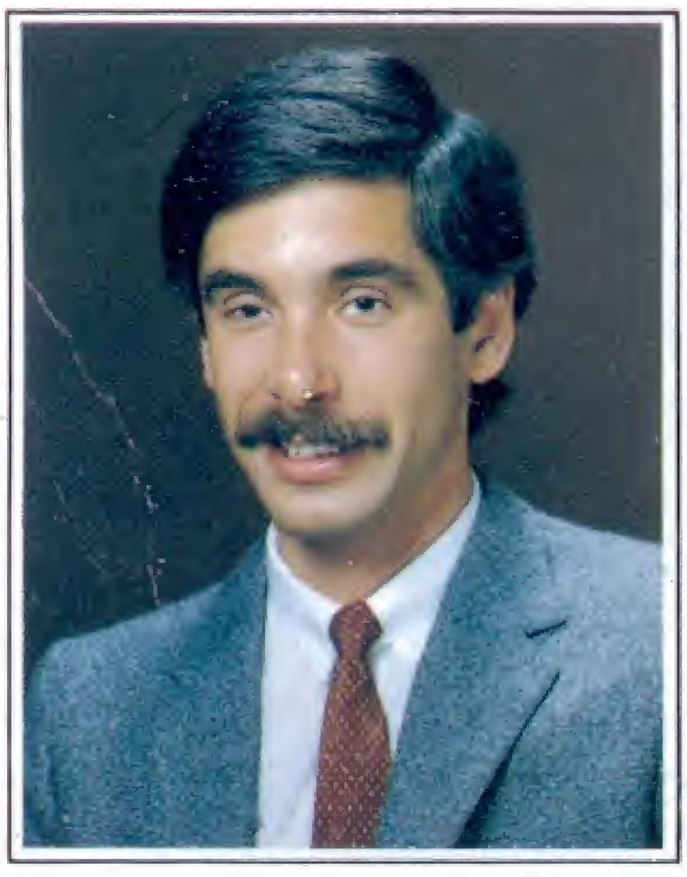
FOR EVERYONE WHO HAS OR WILL HAVE A COMPUTER SYSTEM

DON'T! (OR HOW TO CARE FOR YOUR COMPUTER)

will show you the correct way to handle and care for all the elements of a computer system: the processor itself, the CRT terminal, the disk and the printer. You'll also find recommendations for what to do when something doesn't work, as well as safety and security precautions.

DO READ DON'T if you want to insure continued reliable operation of your system.

ABOUT THE AUTHOR



Dr. Rodnay Zaks, president of Sybex, Inc., has a PhD in Computer Science from the University of California, Berkeley. He has been responsible for the design and installation of computers for industrial control, educational and scientific applications, as well as business and home use. He is the author of numerous books on all facets of computers, including the best selling YOUR FIRST COMPUTER.

ISBN 0-89588-065-2